ETSI TR 101 567 V1.1.1 (2016-01)

Lawful Interception (LI);
Cloud/Virtual Services for Lawful Interception (LI)
and Retained Data (RD)

Reference
DTR/LI-00084

Keywords
cloud, lawful interception, virtual services,
security, retained data

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members** and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are or may be or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Lawful Interception (LI).

The present document does not in any matter establish or imply legal obligations to meet specified LI capability obligations for Cloud/virtual service providers.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document provides an overview of Cloud/virtual services and studies. This includes Lawful Interception (LI) and Retained Data (RD) aspects of these services in the converged Cloud/virtual service environment, the challenges and obstacles of complying with those obligations, what implementations can be achieved under existing ETSI LI standards and what new work may be required to achieve needed Lawful Interception capabilities.

Cloud Services, in whichever forms they take (Infrastructure, Software, Platform or combinations of these), are often trans-border in nature and the information required to maintain LI and RD capability or sufficient coverage for LI/RD support may vary in different countries or within platforms of different security assurance levels. The present document aims to ensure capabilities can be maintained while allowing business to utilize the advantages and innovations of Cloud Services and was undertaken cooperatively with relevant Cloud security technical bodies.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area. .

[i.1] ETSI TS 101 331: "Lawful Interception (LI); Requirements of Law Enforcement Agencies".

[i.2] ETSI TS 101 671: "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".

NOTE: Periodically ETSI TS 101 671 is published as ETSI ES 201 671. A reference to the latest version of the TS as above reflects the latest stable content from ETSI/TC LI.

[i.3] ETSI TS 102 232-1: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery".

[i.4] ETSI TS 102 232-2: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 2: Service-specific details for messaging services".

[i.5] ETSI TS 102 232-3: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 3: Service-specific details for internet access services".

[i.6] ETSI TS 102 232-4: "ETSI TS 101 232-4: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 4: Service-specific details for Layer 2 services".

[i.7] ETSI TS 102 232-5: "ETSI TS 101 232-5: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 5: Service-specific details for IP Multimedia services".

[i.8] ETSI TR 103 690: "Lawful Interception (LI); eWarrant Interface".

[i.9] Special Publication 800-145: "The NIST Definition of Cloud Computing", Sept 2011.

[i.10] NIST SP 800-144: "Guidelines on Security and Privacy in Public Cloud Computing".

[i.11] ETSI TS 133 106: "3G security; Lawful interception requirements".

[i.12] ETSI TS 133 107: "3G security; Lawful interception architecture and functions".

[i.13] ETSI GS NFV 002: "Network Functions Virtualisation (NFV); Architectural Framework".

[i.14] ETSI GS NFV 003: "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

[i.15] ETSI TR 121 905: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Vocabulary for 3GPP Specifications (3GPP TR 21.905)".

[i.16] ETSI NFV ISG: "Network Functions Virtualisation" - Update White Paper, October 2013.

NOTE: This white paper is available at: http://portal.etsi.org/NFV/NFV_White_Paper2.pdf.

[i.17] ETSI GS NFV 001: "Network Functions Virtualisation (NFV); Use Cases".

[i.18] Recommendation ITU-T X.1546: "Malware attribute enumeration and characterization".

[i.19] ETSI TS 133 108: "Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Handover interface for Lawful Interception (LI) (3GPP TS 33.108)".

[i.20] ITU-T Focus Group on Cloud Computing Technical Report, Part 2: Functional requirements and reference architecture (02/2012).

[i.21] ITU-T Technical Report Part 3: "Cloud/virtual network infrastructure model (ITU-T Cloud TR3)".

[i.22] NIST Cloud Computing Reference Architecture: Recommendations of the National Institute of Standards and Technology (Special Publication 500-292).

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions given in ETSI TR 121 905 [i.15] and the following apply:

appliance: self-contained IT system that can be plugged into an existing IT infrastructure to carry out a single purpose

application virtualization: virtual implementation of the application programming interface (API) that a running application expects to use

authentication: verifying the identity of a user, process or device, often as a prerequisite to allowing access to resources in an information system

broad network access: capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g. mobile phones, tablets, laptops and workstations)

Cloud communication centre: service that enables advanced features for the customer-enterprise interaction using the communication and management capabilities provided by a Cloud based telecommunication infrastructure (managed by the Cloud service provider)

Cloud computing: model for enabling service user's ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction

NOTE: Cloud computing enables Cloud services.

Cloud federation: manner to implement inter-Cloud computing in which mutually trusted clouds logically join together by integrating their resources

NOTE: Cloud federation allows a Cloud service provider to dynamically outsource resources to other Cloud service provider in response to demand variations.

Cloud infrastructure: basis of a Cloud, which provides capabilities for computing, storage and network resources, including resource orchestration, virtualization and sharing

NOTE: It also provides relevant cross layer supporting functions to support the upper layer Cloud services as well.

Cloud Lawful Interception Function (CLIF): architecture or system in a Cloud virtualization environment that provides for the instantiation of LI capabilities including receiving and responding to structured expressions for LEA Lawful Interception production requests

Cloud platform: set of capabilities to develop and enable Cloud Services utilizing information technology and communication resources. Some combinations of platform functionalities can be provided as Cloud services

Cloud service: service that is delivered and consumed on demand at any time, through any access network and using any connected devices using Cloud computing technologies

Cloud service partner (CSN): person or organization who provides support to Cloud service provider's service offer building (e.g. service integration)

CLoud Service Provider (C(L)SP): provider that provides and/or maintains Cloud services

Cloud Service User (CSU): person or organization that consumes Cloud services

NOTE: End-users can be persons, machines, applications.

Communications as a Service (CaaS): category of Cloud services where the capability provided to the Cloud service user is to use real time communication and collaboration services (this includes voice over IP, instant messaging, video conferencing, for different user devices)

community Cloud: Cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g. mission, security requirements, policy and compliance considerations)

NOTE: It may be owned, managed and operated by one or more of the organizations in the community, a third party or some combination of them and it may exist on or off premises.

compliance: act of adhering to and demonstrating adherence to, a standard or regulation

control: ability to decide, with high confidence, who and what is allowed to access subscriber data and programs and the ability to perform actions

Data as a Service (DaaS): category of Cloud services where a service provides access to data on user demand regardless of geographic or organizational separation of provider and consumer

NOTE: DaaS includes the capability of presenting the data in the form and structure required by the consumer rather than requiring extensive knowledge of the underlying physical data form and structure.

hybrid Cloud: Cloud infrastructure is a composition of two or more clouds (private, community or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g. Cloud bursting for load-balancing between clouds)

NOTE: It should be noted that the Cloud deployment models do not reflect where services, platforms, applications, resources are actually hosted. For example, a private Cloud can be hosted internally (on-site) or externally (outsourced).

hypervisor: virtualization component that manages the guest OSs on a host and controls the flow of instructions between the guest OSs and the physical hardware

Infrastructure as a Service (IaaS): computing resources (generally hardware) provided by the Cloud service provider to allow the consumer to run consumer provided software including operating systems

NOTE: The capability provided to the consumer is to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying Cloud infrastructure but has control over operating systems, storage and deployed applications; and possibly limited control of select networking components (e.g. host firewalls).

instantiation: creation of a real instance or particular realization of an abstraction or template such as a class of objects or a computer process

NOTE: To instantiate is to create such an instance by, for example, defining one particular variation of object within a class, giving it a name and locating it in some physical place.

inter-Cloud computing: on-demand reassignment of Cloud resources including compute, storage and network and transfer of workload through interworking of Cloud systems

inter-Cloud federation: manner to implement inter-Cloud computing in which mutually trusted clouds logically join together by integrating their resources

NOTE: Inter-Cloud federation allows a C(L)SP to dynamically outsource resources to other C(L)SPs in response to demand variations.

inter-Cloud peering: direct inter-connection between two C(L)SPs

Inter-Cloud Service Broker (ISB): indirect interconnection between two (or more) C(L)SPs achieved through an interconnecting C(L)SP which, in addition to providing interworking service functions between the interconnected C(L)SPs, also provides brokering service functions for one (or more) of the interconnected C(L)SPs

NOTE 1: ISB also covers the case in which one (or more) of the interconnected entities receiving brokering service is a Cloud service user (CSU).

NOTE 2: Brokering service functions generally include, but are not limited to, the following three categories: service intermediation, service aggregation and service arbitrage.

measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g. storage, processing, bandwidth and active user accounts)

NOTE: Resource usage can be monitored, controlled and reported, providing transparency for both the Cloud service provider and Cloud service user of the utilized service.

multi-tenancy: characteristic of Cloud in which resources are shared amongst multiple Cloud tenants

Network Function (NF): functional building block within a network infrastructure, which has well-defined external interfaces and a well-defined functional behaviour

NOTE: In practical terms, a Network Function is today often a network node or physical appliance.

NFV Infrastructure (NFVI): totality of all hardware and software components which build up the environment in which VNFs are deployed

NOTE 1: The NFV-Infrastructure can span across several locations, i.e. multiple N-PoPs. The network providing connectivity between these locations is regarded to be part of the NFV-Infrastructure.

NOTE 2: N-PoP is defined as Network Point of Presence.

Network as a Service (NaaS): category of Cloud services where the capability provided to the Cloud service user is to use transport connectivity services and/or inter-Cloud network connectivity services

NOTE: NaaS services include flexible and extended VPN, Bandwidth on demand, etc.

on-demand self-service: Cloud service user can unilaterally provision computing capabilities, such as server time, network storage and communication and collaboration services, as needed automatically without requiring human interaction with each service's Cloud service provider

orchestration: orchestration refers to combining multiple automation tasks to provision the network, storage array, storage area network, firewalls, hypervisor, operating system and even the application

partitioning: managing guest operating system access to hardware so that each guest OS can access its own resources but cannot encroach on the other guest OSs' resources or any resources not allocated for virtualization use

Platform as a Service (PaaS): hardware and software resources and tools allowing consumer to deploy consumer created or acquired applications using programming languages, libraries, services and tool provided by the Cloud service provider

NOTE: The capability provided to the consumer is to deploy onto the Cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services and tools supported by the provider. The consumer does not manage or control the underlying Cloud infrastructure including network, servers, operating systems or storage, but has control over the deployed applications and possibly the application-hosting environment.

private Cloud: Cloud infrastructure is operated solely for exclusive use by a single organization comprising multiple consumers (e.g. business units)

NOTE: It may be owned, managed or operated by the organization, a third party or some combination of them.

public Cloud: Cloud infrastructure provisioned for open use by the general public

NOTE: It may be owned, managed or operated by a business, academic or government organization or some combination of them.

resource: any kinds of resources to be shared to compose Cloud services including computing power, storage, network, database and applications

service: component of the portfolio of choices offered by service providers to a user, a functionality offered to a user, as defined in ETSI TR 121 905 [i.15]

NOTE: A user may be an end-customer, a network or some intermediate entity.

service aggregation: combines and integrates multiple services into one or more new services

NOTE: It ensures that data are modelled across all component services and integrated, as well as ensures the movement and security of data between the Cloud service user and multiple Cloud service providers.

service arbitrage: similar to the service aggregation capability

NOTE: The difference between them is that the services being aggregated are not fixed. Indeed, the goal of arbitrage is to provide flexibility and opportunistic choices for the service aggregator, e.g. providing multiple e-mail services through one Cloud service provider or providing a credit-scoring service that checks multiple scoring agencies and selects the best score.

Service Delivery Platform: system architecture or environment that enables the efficient creation, deployment, execution orchestration and management of one or more classes of services

service intermediation: service that directly enhances a given service delivered to one or more Cloud service users, essentially adding value on top of a given service to enhance some specific capability

Software as a Service (SaaS): allows the consumer to use Cloud service provider's applications

NOTE: The applications are shared, but the consumer may have private application specific data such as application configuration settings. The capability provided to the consumer is to use the provider's applications running on a Cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g. web-based email) or a program interface. The consumer does not manage or control the underlying Cloud infrastructure including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

user service: component of the portfolio of choices offered by service providers to the end-users/customers/subscriber

Virtual Data Centre (VDC): evolutionary computing model that presents the data centre as a service view to a single computer, which virtualizes all hardware and software resources behind it

Virtual Desktop as a Service (VDaaS): capability provided to the Cloud service user to use virtualized desktops from a Cloud service provider in the form of outsourcing

NOTE: VDaaS is also called virtual desktop or hosted desktop services, is the outsourcing of virtual desktop infrastructure (VDI). The consumer's personal data is copied to and from the virtual desktop during login/logoff and access to the desktop is device, location and network independent. The virtual desktop can be delivered either through a client-server model or through a web interface.

virtual hardware: hardware (including the CPU, controllers, Ethernet devices and disks) that is seen by the guest software

virtual machine: complete environment that supports the execution of guest software

NOTE 1: A virtual machine is a full encapsulation of the virtual hardware, virtual disks and the metadata associated with it

NOTE 2: Virtual machines allow multiplexing of the underlying physical machine through a software layer called a hypervisor.

Virtualized Network Function (VNF): implementation of an NF that can be deployed on a Network Function Virtualization Infrastructure (NFVI)

virtualization: simulation of the software and/or hardware upon which other software runs

3.2 Abbreviations

For the purposes of the present document, the following terms and definitions given in ETSI TR 121 905 [i.15] and the following apply:

AAA	Authentication, Authorization, and Audit
AMQP	Advanced Message Queuing Protocol
ANDSF	Access Network Discovery and Selection Function
ANSDF	Access Network Discovery and Selection Function
API	Applications Programming Interface
APN	Access Point Name
ARC	Architecture Working Group
ARTS	Association for Retail Technology Standards
ASP	Application Service Provider
ATIS	Alliance for Telecommunications Industry Solutions (US)
AWS	Amazon Web Services
BCASR	Broadcasting Working Group
BCP	Business Continuity Plan
BI	Business Intelligence
BMC	BMC Software
BOF	Birds of a Feather
BSS	Business Support System
BYOD	Bring your own device
C(L)SP	Cloud Service Provider
CA	CA Technologies

CA/B	Certificate of Authority/Browser Forum
CaaS	Communications as a Service
CAI	Consensus Assessments Initiative Working Group
CC	Call Content
CCDB	Common Criteria Development Board
CCEA	Cloud Computing Experts Association
CCI	Cloud Computing Infrastructure
CCIF	Content of Communication Interception Function
CCM	Cloud Controls Matrix Working Group
CCSA	China Communications Standards Association
CD	Content Delivery Working Group
CDG	Cloud Data Governance Working Group
CDMI	Cloud Data Management Interface
CIE	Chinese Institute of Electronics
CII	Communication-Identifying Information
CIM	Common Information Model
CLIF	Cloud Lawful Interception Function
COM	Communications Working Group
CPU	Central Processing Unit
CPWG	Cloud Profiles Working Group
CSA	Cloud Security Alliance
CSB	Cloud Service Broker
CSCC	Cloud Standards Customer Council
CSCF	Call Service Control Function
CSI	The Cloud Storage Initiative
CSN	Cloud Service Partner
CSP	Communication Service Provider
CSP/C	Communications Service Provider / Cloud
CSR	Cloud Service Requester
CSU	Cloud Service User
CTP	CloudTrust Protocol Working Group
DaaS	Data as a Service
DAPS	Distributed application platforms and services
DHCP	Dynamic Host Configuation Protocol
DM	Device Management Working Group
DMTF	Distributed Management Task Force
DNS	Directory Name Service
DPCO	Data Protection and Capacity Optimization Committee
DRAM	Dynamic random-access memory
DRM	Digital Rights Management Working Group
DSaaS	Data Storage as a Service
DSL	Digital Subscriber Line
DT	Dynamic Triggering
ENISA	European Network and Information Security Agency
ESF	Ethernet Storage Forum
FQDN	Full Qualified Domain Name
FTP	File Transfer Profile
GICTF	Global Inter-Cloud Technology Forum
GRC	GRC Stack Working Group
GS	Group specification
GSC	Global Standards Collaboration
GSI	Green Storage Initiative
GSMA	Global System for Mobile Communications (GSM) Association
GUP	3GPP Generic User Profile
HI	Handover Interface
HIM	Health Information Management Working Group
HP	HP Cloud Services
HSS	Home Subscription Server
HTTP	Hyper Text Transfer Protocol
IaaS	Infrastructure as a Service
IAP	Intercept Access Point
IBM	International Business Machines

ICT	Information and Communication Technologies
ICWG	Intercloud Working Group
IDC	Internet Data Centre
IdM	Identity management
IED	Information Element Data
IETF	Internet Engineering Task Force
IM	Instant Message
IMS	IP Multimedia Subsystem
IMSI	GSM International Mobile Subscriber Identity
IOP	Interoperability Working Group
IoT	Internet of Things
IP	Internet Protocol
IPC	Inter Process Communication
IPTV	Internet Protocol Television
IRI	Information Related to Interception
ISB	Inter-cloud Service Broker
ISMP	Inter-System Mobility Policy
ISP	Internet Service Provider
ISRP	Inter-System Routing Policy
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
LIaaS	Lawful Interception as a Cloud Service
LOC	Location Working Group
LTE	Long Term Evolution
M2M	Machine to Machine
MAEC	Malware Attribute Enumeration and Characterization
MCP	Mobile Cloud Provider
MME	Mobile Management Entity
MNO	Mobile Network Operator
MSC	GSM Mobile-services Switching Centre
MTM	Mobile Phone Work Group
MWG	Cloud Metrics Working Group
NaaS	Network as a Service
NF	Network Function
NFVI	NFV Infrastructure
NGN	Next Generation Networks
NII	Network Independent Interface
NIST	National Institute of Standards and Technology
NNI	Network Network Interface
N-PoP	Network Point of Presence
OAM	Operation and maintenance
OASIS	Organization for the Advancement of Structured Information Standards
OCC	Open Cloud Consortium
OCCI	Open Cloud Computing Interface
OCSD	Open Science Data Cloud Working Group
ODCA	Open Data Center Alliance
OGF	Open Grid Forum
OMA	Open Mobile Alliance
OMG	Object Management Group
OS	Operating System
OSS	Operations Support System
OTT	Over-the-Top
OTTF	Open Group Trusted Technology Forum
OVF	Open Virtualization Format
PaaS	Platform as a Service
PDG	Packet Data Gateway
PGP	Pretty Good Privacy
PGW	PDN Gateway
PMRM	Privacy Management Reference Model
PSIG	Platform Special Interest Group
PSTN	Public Switched Telecommunication Network

QoS	Quality of Service
RAM	Ramdom Access Memory
RDaaS	Retained Data as a Cloud Service
RDBMS	Relational Database Management System
REL	Release Planning and Management Committee
REQ	Requirements Working Group
RGW	Residential GateWay
SaaS	Software as a Service
SAJACC	Standards Acceleration to Jumpstart the Adoption of Cloud Computing Working Group (NIST)
SAS	Statements on Auditing Standards
SBC	Session Border Controller
SCAP	Security Content Automation Protocol
SDN	Software defined network
SDP	Service Delivery Platform
SDPaaS	SDP as a Service
SGW	Security Gateway
SID	Information Framework Domain
SIRT	Security Incident Response Team
SLA	Service Level Agreement
SMB	Small Medium Business
SMI	Storage Management Initiative
SMS	GSM Short Message Service
SMTP	Simple Mail Transfer Protocol
SNIA	Storage Networking Industry Association
SOA	Service Oriented Architecture
SON	Self Organising Networks
SOP	Service Orchestration and Desciption for Cloud Services
SP	Service Provider
SSD	Service Specific Delivery
SSID	Service Set IDentifier
SSIF	Storage Security Industry Forum
SSL	Secure Socket Layer
TAM	Application Framework Domain
TAS	Telephony Application Server
TC	Technical Committee
TCG	Trusted Computing Group
TCI	Trusted Cloud Initiative Working Group
TMI	Trusted Multi-tenant Infrastructure Work
TNC	Trusted Network Connect Work Group
TOSCA	Topology and Orchestration Specification for Cloud Applications
TPM	Trusted Platform Module Work Group
TSAG	Telecommunication Standardization Advisory Group
TSP	TelepreSence Provider
TSS	TCG Software Stack Work Group
TTP	Trusted Third Party
TWG	Telecom Working Group
UE	(3GPP) User Equipment
URI	Uniform Record Identifier
URL	Unified Resource Locator
US	United States
VDaaS	Virtual Desktop as a Service
VDC	Virtual Data Centre
VDI	Video Device Interface
VIM	Virtual Infrastructure Manager
VLAN	Virtual Local Area Network
VM	Virtual Machine
VMI	Virtual Machine Image
VMM	Virtual Machine Manager
VNF	Virtualised Network Function
VNO	Virtual Network Operator
VO	Visited Operator
VoLTE	Voice over LTE

VPN	Virtual Private Network
VPWG	Virtualized Platform Work Group
WG	Working Group
WLAN	Wireless LAN
XAM	XAM Initiative
XDA	XDA Developers Forum
XML	eXtensible Mark up Language

4 Cloud Services Overview

4.1 Introduction

Cloud services are very diverse and constantly evolving. Work is on-going in many different industry standards forums listed in annex B on service conceptualization, reference architectures, infrastructure models and resource management. Many of the service definitions that have achieved a level of stability are included in clause 3. This clause provides an overview on Cloud/virtual services.

Figure 4-1 provides a model of the Cloud ecosystem that depicts the relationships amongst the three major players in the present document: users/subscribers, the Cloud service providers and traditional/communication service providers with whom the users/subscribers may have a commercial relationship. Cloud service providers and communication service providers may also have a commercial relationship independent of those with the users/subscribers.

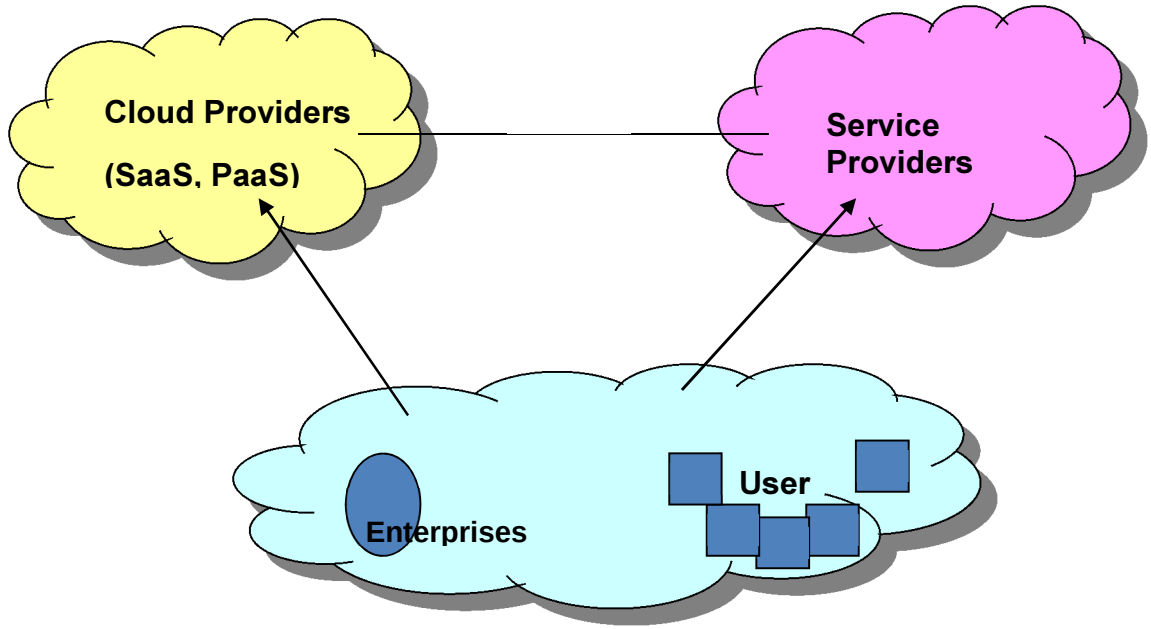


Figure 4-1: Cloud Ecosystem

4.2 Perspectives on Cloud services

4.2.1 Introduction

Cloud computing, including distributed virtual services, is an evolving paradigm that is fundamentally and rapid changing communication services and infrastructure.

The diversity of these services and the underlying infrastructure has itself produced different perspectives.

In general, most of the many forums dealing with Cloud computing have found common ground in the following description (Special Publication 800-145, The NIST Definition of Cloud Computing, Sept 2011 [i.9]):

"Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This Cloud model promotes availability and is composed of five essential characteristics, three service models and four deployment models."

4.2.2 General characteristics of Cloud services

On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g. mobile phones, tablets, laptops and workstations).

Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. Cloud services are location independent. The customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g. country, state or data centre). Examples of resources include storage, processing, memory, network bandwidth and virtual machines.

Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service: Cloud systems control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g. storage, processing, bandwidth and active user accounts). Resource usage can be monitored, controlled and reported, providing transparency for both the provider and consumer of the utilized service.

4.2.3 Service models for Cloud services

Cloud computing enables hardware and software to be delivered as "services" that are provided on demand or sold on a usage basis. The following are common service models, which are defined in detail in clause 3.1:

- Communications as a Service (CaaS)
- Data as a Service (DaaS)
- Infrastructure as a Service (IaaS)
- Network as a Service (NaaS)
- Platform as a Service (Paas)
- Software as a Service (Saas)
- Virtual Desktop as a Service (VDaaS)

4.2.4 Deployment models for Cloud services

Private Cloud: The Cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g. business units). It may be owned, managed and operated by the organization, a third party or some combination of them and it may exist on or off premises.

Community Cloud: The Cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g. mission, security requirements, policy and compliance considerations). It may be owned, managed and operated by one or more of the organizations in the community, a third party or some combination of them and it may exist on or off premises.

Public Cloud: The Cloud infrastructure is provisioned for open use by the general public. It may be owned, managed and operated by a business, academic or government organization or some combination of them. It exists on the premises of the Cloud provider.

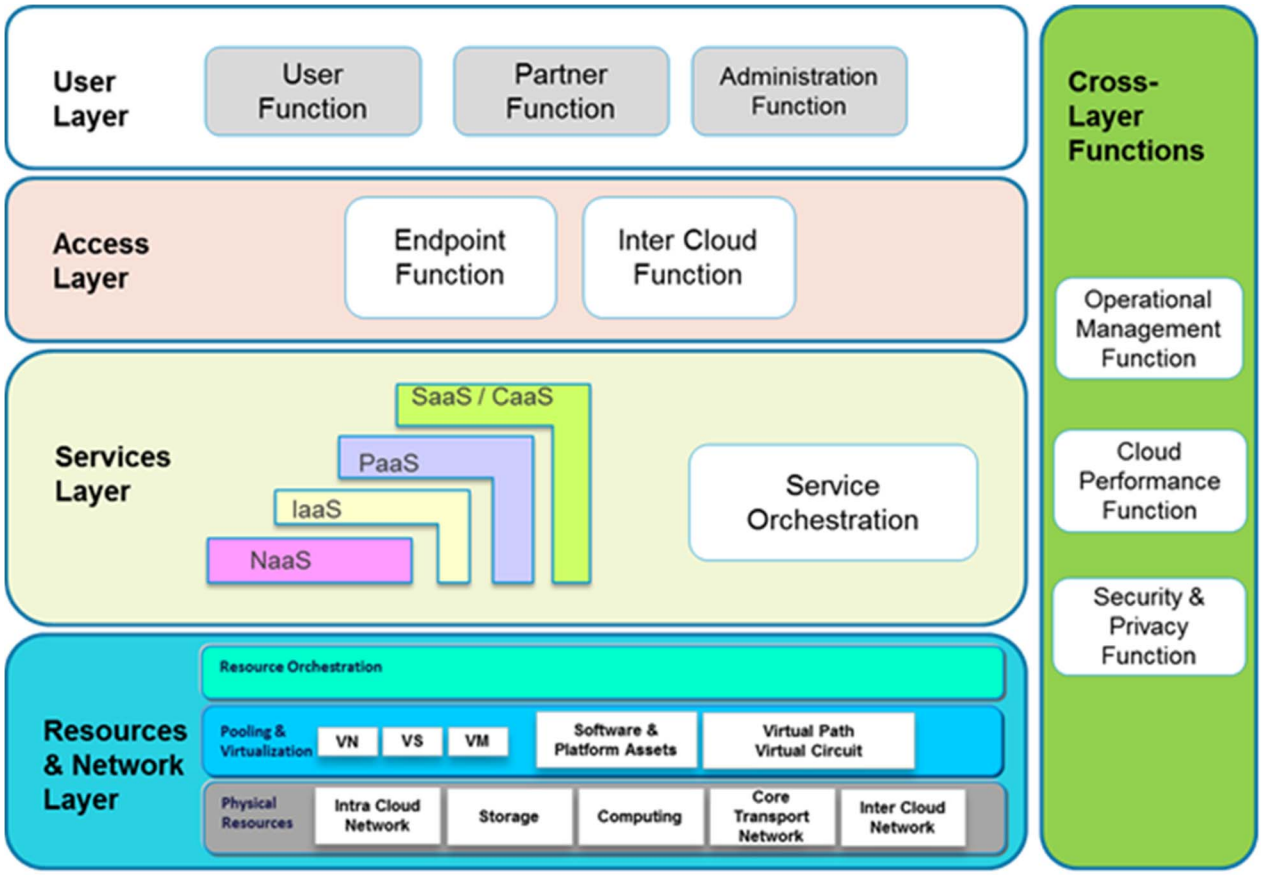
Hybrid Cloud: The Cloud infrastructure is a composition of two or more distinct Cloud infrastructures (private, community or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g. Cloud bursting for load balancing between clouds).

4.3 Cloud reference architectures and infrastructures

The Cloud architecture meets several needs to enable sustained innovation and development of Cloud services. With multiple stakeholders involved, the Cloud architecture be flexible to fit the needs of infrastructure C(L)SPs, CSPs and service resellers. The following high-level needs are broadly envisioned for the Cloud architecture:

- Support for many standards within the same Cloud infrastructure and allow for evolution of these standards, without requiring disruptive infrastructure changes.
- Broadband access.
- The Cloud architecture enables multiple current and future deployment models, Cloud service categories and use cases, in whole or in part.
- For private and hybrid Cloud operations, Cloud services need to appear like intranet services.
- Early detection, diagnosis and fixing of infrastructure or service-related problems.
- Auditing and compliance, including service-level monitoring of resources allocated to users.
- Invisibility of Cloud resource allocations to Cloud service users. A C(L)SP may choose to expose service-operation details without having to share Cloud internal infrastructure allocation and provisioning details for security and business reasons, including meeting LI needs.
- Users consuming Cloud services are able to control Cloud resource access to the CSP transparently and enable IT procedures to work without compromise in legal or organizational mandates.
- Intranet-level security capabilities that may include access records, activity reports, session monitoring, firewalling, access control and malicious attack detection and prevention.
- Resource mobility which includes virtual machine mobility.
- Resource scalability.
- Naming identity management.
- Automated resource deployments.

Cloud computing reference architectures typically make use of a framework that defines the layers of a Cloud functional architecture derived by grouping Cloud related functions, see Figure 4-2.



Source: ITU-T Focus Group on Cloud Computing Technical Report, Part 2: Functional requirements and reference architecture (02/2012) [i.20].

Figure 4-2: Cloud related functions

The user layer performs interaction between the Cloud service user and the Cloud infrastructure. The user layer is used to set up a secure mechanism with the Cloud, to send Cloud service requests to the Cloud and receive Cloud services from the Cloud, perform Cloud service access and administrate and monitor Cloud resources.

The access layer provides a common interface for both manual and automated Cloud service capabilities and service consumption. The access layer accepts Cloud service consumption requests using Cloud APIs to access services and resources.

The services layer is where services are orchestrated and exposed in the five Cloud service categories. The resources and network layer is where the physical resources reside. Five categories are typical: Communication as a Service, Software as a Service, Platform as a Service, Infrastructure as a Service and Network as a Service.

Cross-layer functions perform overall system management (i.e. operations, administration, maintenance and provisioning and monitoring, including secure mechanisms.

One architecture dimension that is unique to the Cloud/virtual environment is the concept of the Inter-Cloud function. Cloud services are expected to be offered by C(L)SPs globally and rely on inter-Cloud connections with other C(L)SPs. The inter-Cloud function can be implemented through inter-Cloud peering, inter-Cloud service broker and inter-Cloud federation arrangements.

The Cloud/virtual services reference architecture abstractions are ultimately manifested across multiple network infrastructures as depicted in Figure 4-3.

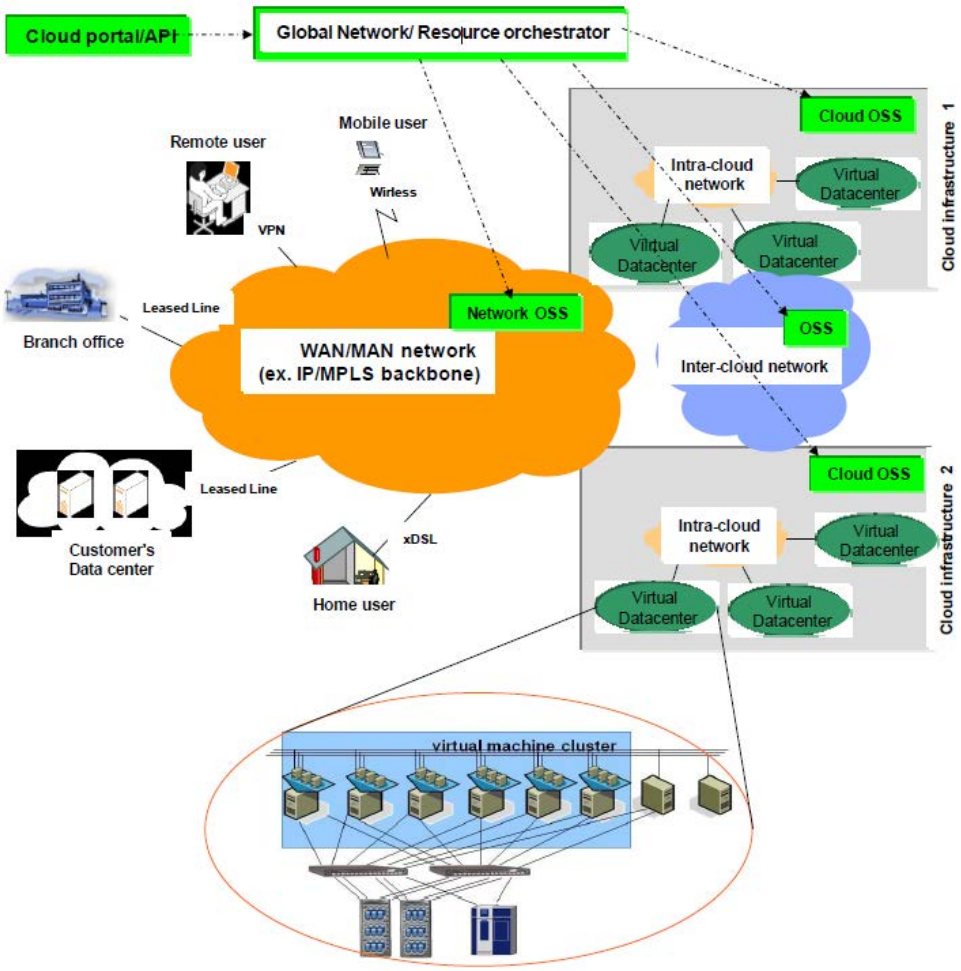


Figure 4-3: Cloud/virtual network infrastructure model (ITU-T Cloud TR3)

These resulting infrastructures in turn enable the far reaching changes being witnessed today. Millions of "app" clients can autonomously provide to many different mobile and fixed end user smart devices that facilitate direct access to tailored services, see Figure 4-4.

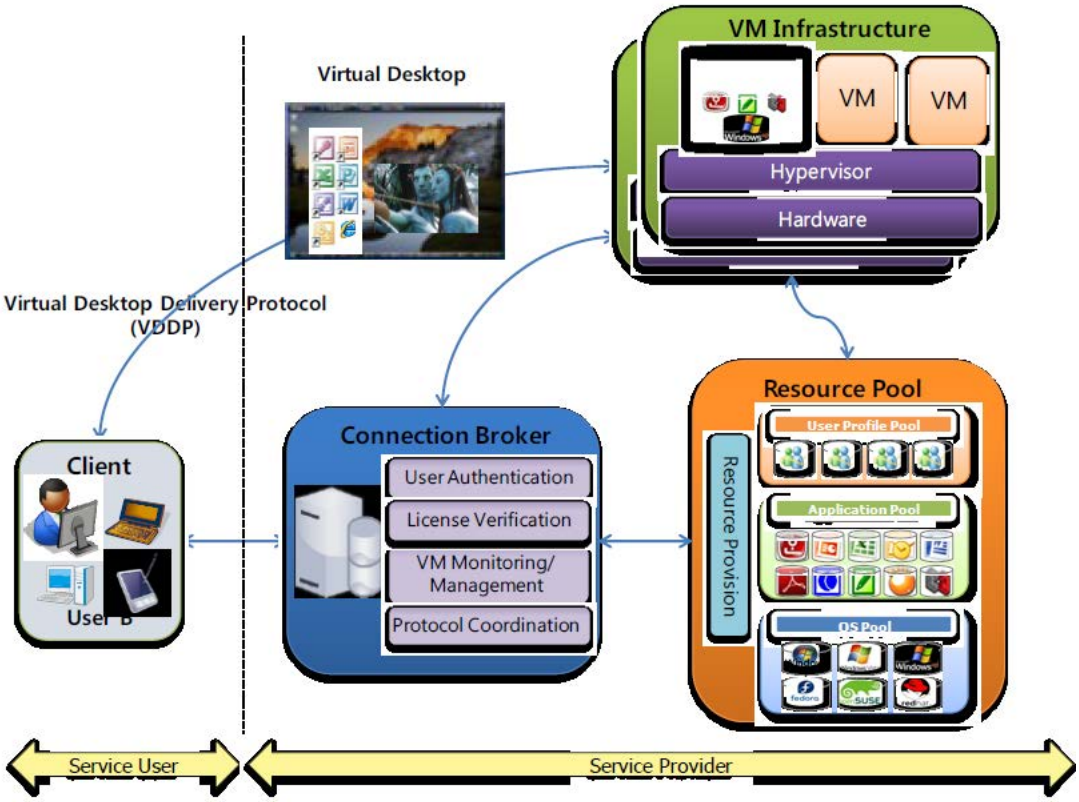


Figure 4-4: Cloud/virtual infrastructure (ITU-T Technical Report Part 2 [i.20], fig. I.1)

4.4 Resource management

Resource management is necessary for maintaining processing, storage and I/O capabilities - physical and virtual - within or across Cloud environments. Cloud infrastructure should provide a unified resource management function for the upper-layers (including virtualized and physical computing resource, storage resource and network resource). The resource management function should provide resource packaging, resource deployment and resource scheduling, whilst managing templates and assets.

Resource packaging provides a unified interface of heterogeneous resource, whether virtualized or physical, to upper-layers for management and utilization. Resource deployment and scheduling provide elastic, dynamic, on-demand and automation management for the down-layers, based on user-defined policies. They also provide resource access control interfaces to the upper-layers and can dynamically allocate the resource by the real-time monitoring of applications and SLAs. Template management provides the capability to describe groups of computing, storage and network resources within their life cycles. Asset management provides unified management of the physical devices, including configuration information and topology of assets.

Resource management is a critical enabler and consists of the ability in a trusted manner to uniquely identify, locate, acquire, format, protect and deliver specific forensics described by a target signature. all these may necessitate an overlay, compartmentalized resource management implementation.

A Cloud resource management model in common use is depicted in Figure 4-5.

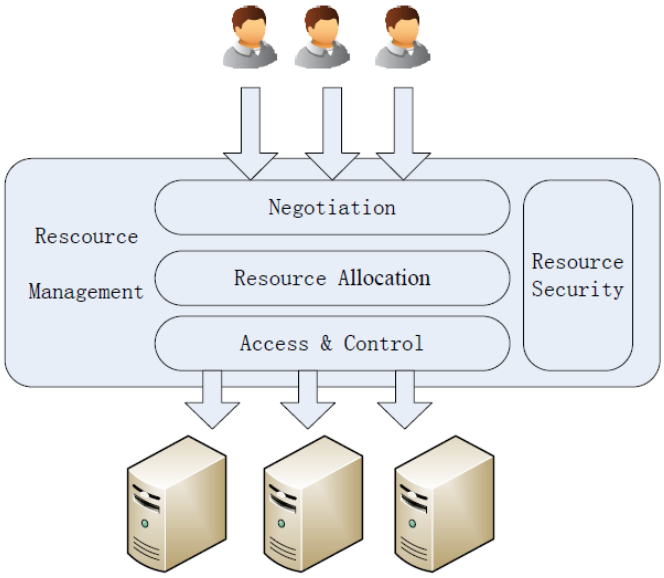


Figure 4-5: Cloud resource management model (ITU-T Technical Report Part 3 [i.21], Fig 11)

An abstract view of the resource management model is shown in Figure 4-6.

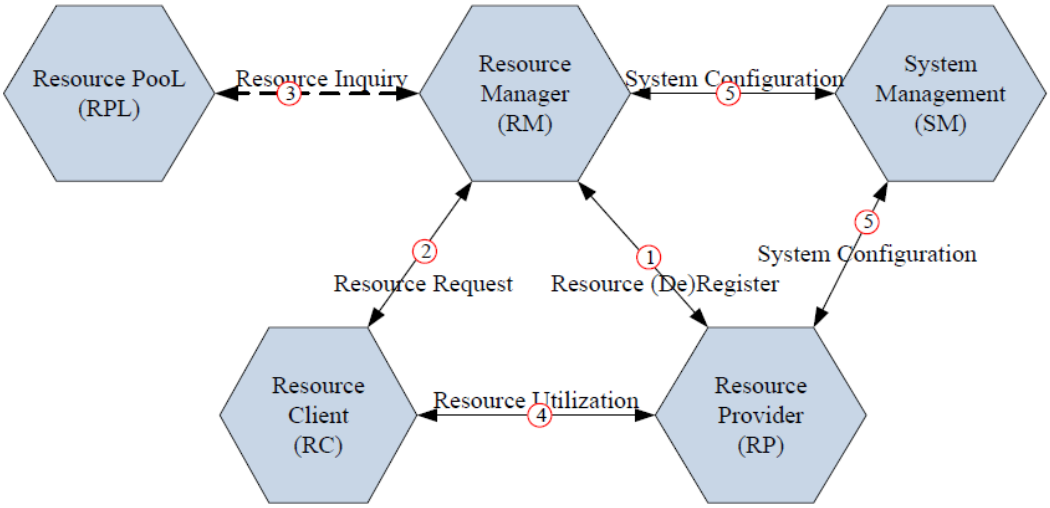


Figure 4-6: Resource management model (ITU-T Technical Report Part 3, Fig 13)

One of the most important of these virtual entities is the Resource Provider. It is the entity which provides and maintains virtualized resources to the resource management platform and is consists of hypervisors.

4.5 Enabling Mobile Cloud

The Cloud ecosystem is already taking shape and a number of players from IT, as well as Over-The-Top (OTT) players already offer agility and scalability through their service offerings.

The fixed and mobile telecommunications network operators have deployed an extensive infrastructure (distributed data centres, broadband access, application servers, etc.) that is ripe for virtualization, allowing these operators to better monetize these resources.

The telecom operators have some important advantages, especially through their existing, strong customer relationship, billing expertise and customer services, which are important for companies wanting to deploy Cloud services.

As such, the operators are in a unique position, especially the mobile operators, to offer a wide variety of bundling of Cloud and network services for customers that practically maintain and expand their business with their existing service provider.

The Mobile Cloud enables existing and new Cloud services to be ubiquitously available across multiple, separate mobile network operator domains.

The Mobile Cloud Providers (MCPs) are the "intermediaries" facilitating the implementation of a Mobile Cloud through agreements with individual network operators (based upon wholesale models).

By using a MCP the Service Providers (SPs) can have a single interface and single business relationship, but interwork with multiple network operators.

From a user's service perspective, one can look at the Cloud environment as an on-demand environment where various services controlled by other organizations can be leveraged and composed for the use of a user, so that the services that are outside of an organization's own boundaries, operated and controlled by other organizations can become part of the aggregated portfolio of services of that organization (e.g. file storage and backup). A Mobile Cloud's example relevant to 3GPP is GSMA's OneAPI's objective is to provide a cross-operator domains framework for Mobile Cloud Computing. Based upon OneAPI, the GSMA is acting as a Mobile Cloud Provider/Aggregator, providing SPs access to network resources and charging capabilities (NaaS type of Cloud) of multiple mobile operators.

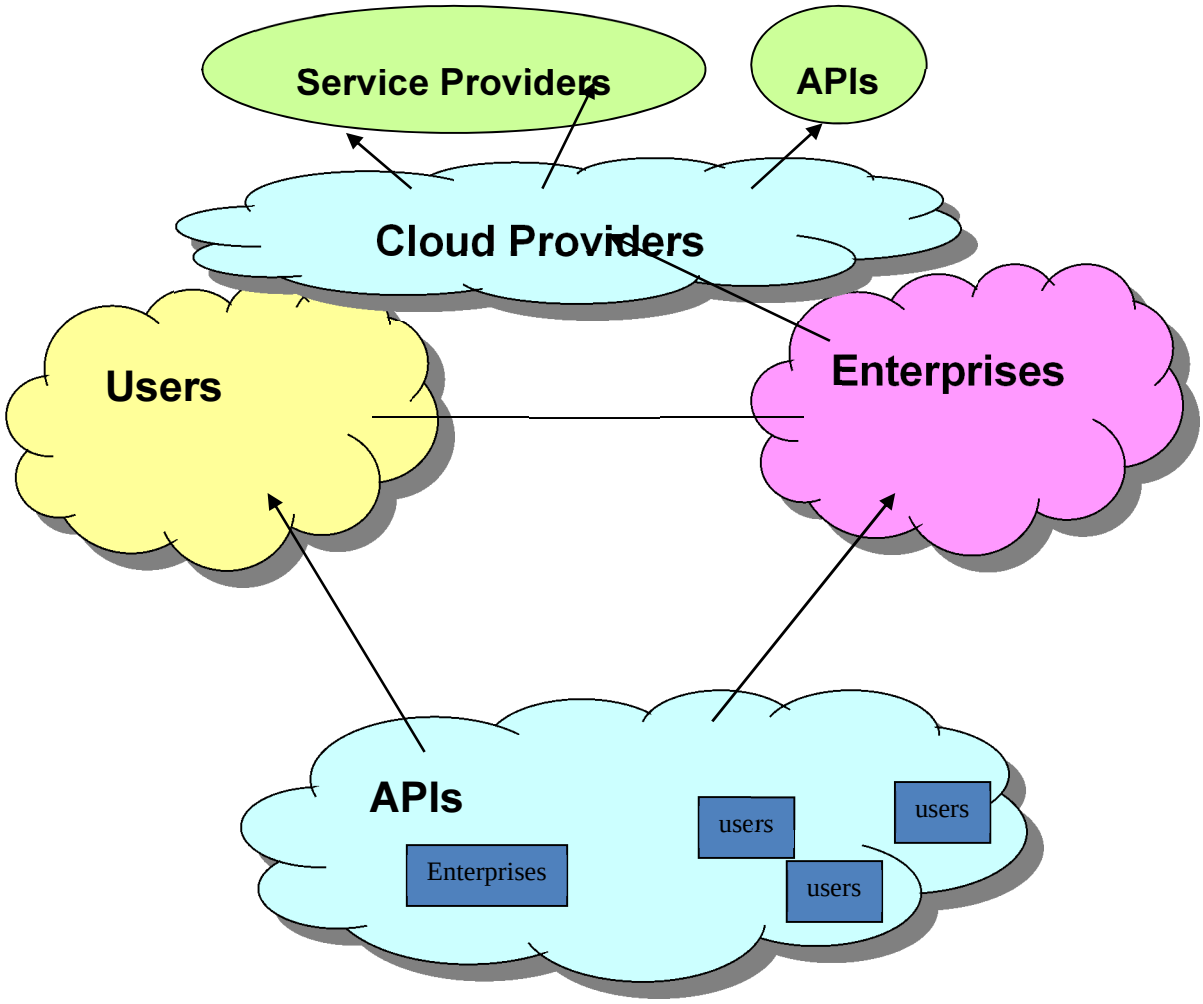


Figure 4-7: Mobile Cloud

5 Network Virtual Services Overview

5.1 Introduction

Virtualized Services, in the present document, refer to the work being studied by ETSI's Network Functions Virtualization Industry Specification Group (NFV ISG). Network Functions Virtualization aims to address operator problems of increasingly complex and proprietary hardware by leveraging standard IT virtualization technology to consolidate many network equipment types onto industry standard high volume servers, switches and storage, which could be located in Datacentres, Network Nodes and in the end user premises. NFV ISG documents can be found at ETSI GS NFV 002 [i.13] and ETSI GS NFV 003 [i.14].

The goal of NFV is to use virtualization to separate network function hardware software. This allows the consolidation of many network equipment types onto industry standard high volume servers, switches and storage. Since Virtualized Network Functions (VNFs) are implemented in software, network operations change as the software can be dynamically moved to or instantiated in, various locations in the network as required, without the need for installation of new equipment. VNF's connection to Cloud computing is that VNFs and the VNF Infrastructure can use Cloud computing's agility and resource sharing.

Traditional network nodes can be considered as a different Network Functions (NFs), which may be virtualized by the CSP. There may be some impacts to LI:

- LI functions may not be taken into consideration.
- LI security may not be taken into consideration, NIST SP 800-144 [i.10].
- Others TBD.

For the purposes of the present document, NFV is virtualizing the network operator's internal functions transparently to their subscribers. Likewise, NFV is complementary to another industry endeavour referred to as Software Defined Networking (SDN), in which control of a function is decoupled from hardware and given to a software application called a controller.

For example, SDN allows network engineers and administrators to monitor and quickly respond to changes in network needs without having to physically touch individual switches. They are able to modify switch rules, such as in traffic prioritization or block specific types of packets with a very precise level of control.

The introduction of NFV results in faster deployments of new network services and greater flexibility to dynamically scale the VNF performance and needed capacity.

Figure 5-1 (from ETSI GS NFV 002 [i.13]), depicts the NFV reference architecture framework. Network functions are software-only entities running on the NFV Infrastructure (NFVI). The NFVI includes diverse physical resources that can be virtualized and supports the execution of the VNFs. The NFV Management and Orchestration handles all the virtualization-specific management tasks necessary and the orchestration and lifecycle management of physical and/or software resources that support the infrastructure virtualization.

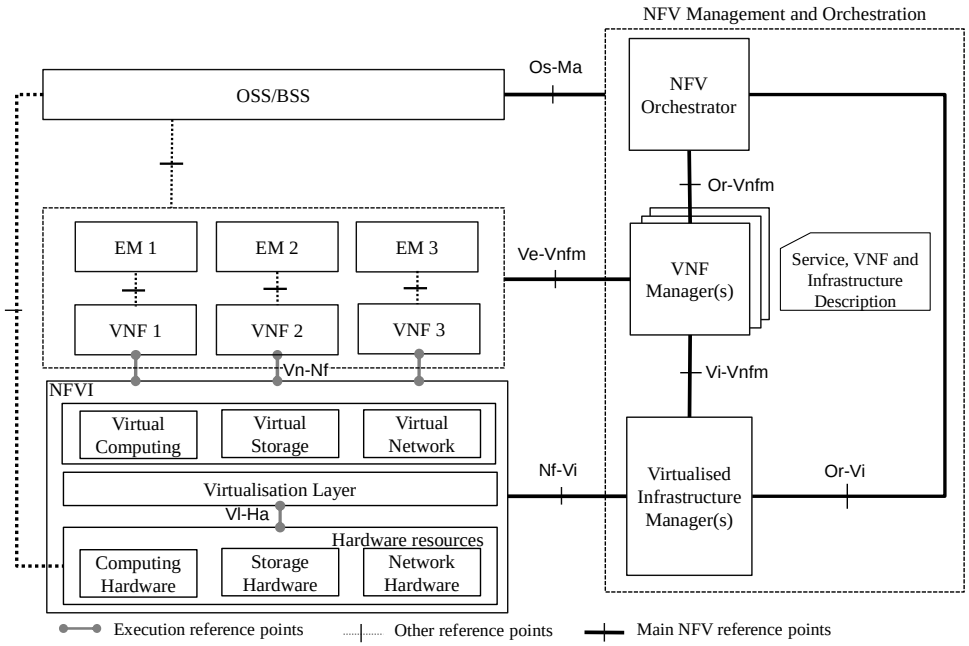


Figure 5-1: NFV reference architectural framework

The decoupling of hardware and software in the network functions is realized by a virtualization layer. This layer abstracts hardware resources of the NFVI. ETSI GS NFV 001 [i.17] includes uses cases and examples of target NFs for virtualization. Some examples of NFs are:

- 3GPP Evolved Packet Core network elements (e.g. Mobility Management Entity MME), Serving Gateway (SGW), Packet Data Network Gateway (PGW)).
- Residential Gateway (RGW) in a home network.
- Conventional network functions such as Dynamic Host Configuration Protocol (DHCP) servers, firewalls, etc.

5.2 NFV relationship to Cloud Services

There are instances in existing networks where network operators have pooled resources (e.g. MSC Pooling); virtualization and Cloud services use the concept of resource pooling as well. Network virtualization allows new business opportunities similar to Cloud service models. A CSP could offer so or all of its NFV Infrastructure as a service to other CSPs. For example, a VNF owner may not necessarily "own" the NFV infrastructure needed for the functioning and operation of the VNF. Since VNFs can be provided by different Service Providers, they may enable an efficient service to global customers.

5.3 NFV standardization

The telecommunications industry uses traditional standardization procedures to develop specifications on which prototyping and testing efforts are based. The information technology industry embraces an "open source" model where a community of developers contribute and integrate pieces of software under terms that facilitate open collaboration and usage. The process of building elements based on these open pieces is driven according to short code-build-test cycles of software prototypes and less stringent agreement rules, based on what has been termed "rough consensus".

In one of their white papers ETSI NFV ISG [i.16], the NFV ISG has stated a preference in using the open source model to progress NFV implementation quickly without being delayed by standardization with the expectation that SDOs will either update existing specifications or quickly create new specifications to ensure interoperability.

6 Lawful Interception

6.1 Introduction

The on-going work in the industry and standards forums dealing with Cloud and virtual services recognize that a broad array of existing legal obligations apply to the services being provided, including lawful interception. This clause describes lawful interception obligations.

6.2 LEA

6.2.1 Identify and communicate with the responsible service providers

The most fundamental need for LEAs is to be able to identify and communicate with the service provider(s) responsible for the communications involving specific targets. Cloud environments are especially challenging because the relevant C(L)SP providers are often not subject to registration, regulatory or CSP partnership needs that facilitate discovery of their identity(ies). Furthermore, the responsible providers' relationships are often complex. For example, relationships are layered, where an application service provider with the direct customer relationship uses a Software-as-a-Service provider that aggregates Infrastructure-as-a-Service resources at a data centre.

6.2.2 Facilitate access and delivery across different jurisdictions

While the legal and regulatory aspects of multi and cross jurisdictional handovers is out of scope of the present document, the implementation of common structured expressions for the eWarrant and handover information can provide the technical underpinnings for facilitating such implementations.

Due to the nomadic access to Cloud services, no one provider (as described in Figure 5-1) is likely to be capable of dealing with all warrants/intercept requests. Because LI obligations are largely oriented around national jurisdiction and geography, it is unlikely that LEAs can serve a warrant on a Cloud provider directly unless that Cloud provider has an "in country" presence.

The specific Cloud resources are generally not important nor should their geographical location - as long as they are within the jurisdiction of the LEA. The following list identifies when a CSP/C(L)SP is able to intercept the traffic on the (local) LEA's behalf:

- The warrant complies with the laws of that country.
- The traffic is present (i.e. it needs to be routed or handled in the same country). Duplication is permitted as is rerouting as long as the user or any other unauthorised party remains unaware of LEA interest.
- It is possible to clearly distinguish this traffic from others (i.e. no collateral interception).
- If the traffic is encrypted, the entity responsible for key management ensures it can be decrypted by the CSP/C(L)SP or LEA.

6.2.3 Existing telecommunications services implemented using Cloud/virtual capabilities

Substantial diversity exists among Cloud facilities and services that affect the nature and implementation of Law Enforcement Agency (LEA) needs. However, if a CSP elects to implement a Cloud service and becomes a C(L)SP, their legal obligation to support LI is unchanged. To the extent relevant, the needs of Law Enforcement Agencies articulated in ETSI TS 101 331 [i.1] still apply. What may be impacted are the technical solutions outlined in ETSI LI standards as the underlying architecture may be changed by the implementation of Cloud services.

The specific Cloud service that is to be intercepted is subject to national laws. National laws may require different levels of capabilities and procedures for LI in public and private networks. Additionally, the definitions of a private network may vary with jurisdictions.

The list below provides examples of the telecommunications services for which there are LI solutions:

- Voice, conferencing, IMS-based services

- Messaging (SMS, E-mail, etc.)
- Internet Access

Other services - most of which are Cloud-based - have no standardized LI solution. This includes services such as file sharing, telepresence, so-called "social networks" or "virtual games". In most countries, there are no existing regulations concerning these services.

6.3 CSP / C(L)SP Provider Obligations

6.3.1 Overview

CSPs typically have a number of responsibilities which can be roughly summarized into two areas:

- Provision and Maintenance of lawful interception capability.
- Protection of information and activities pursuant to this responsibility.

In accordance to national law, CSPs are still responsible to provide the "access" interception capability and "service" interception capability for those services which they offer.

The introduction of NFV does not alter the national obligations of the CSPs/C(L)SPs. However, with the on-going NFV development, it is unclear how LI functionality will be realized in the NFV environment.

C(L)SPs and Cloud facility operators are subject to many legal and regulatory obligations that vary among the jurisdictions in which they have physical presence or offer service. Service agreements among C(L)SPs and with CSPs may also impose additional obligations.

National regulations may determine if and which type of Cloud providers (e.g. CaaS, IaaS, PaaS, SaaS) will be subject to lawful interception obligations. National regulations may determine other means to identify which Cloud providers have lawful interception obligations (e.g. by specific service provided). Some Cloud providers may have an obligation because they offer a particular user service identified in that nation as required to be intercepted but other Cloud providers would not have a similar obligation if they do not offer services specifically identified.

Trusted Third Parties (TTPs) may also provide support for some of those obligations by service agreement and local/national law.

In most jurisdictions, CSPs or their designated TTP support law enforcement requests for lawful interception in a timely fashion and in a manner that complies with the law and other obligations of that jurisdiction. See clause 6.2.1.

A generic overview of how CSP's view interception responsibilities is described below.

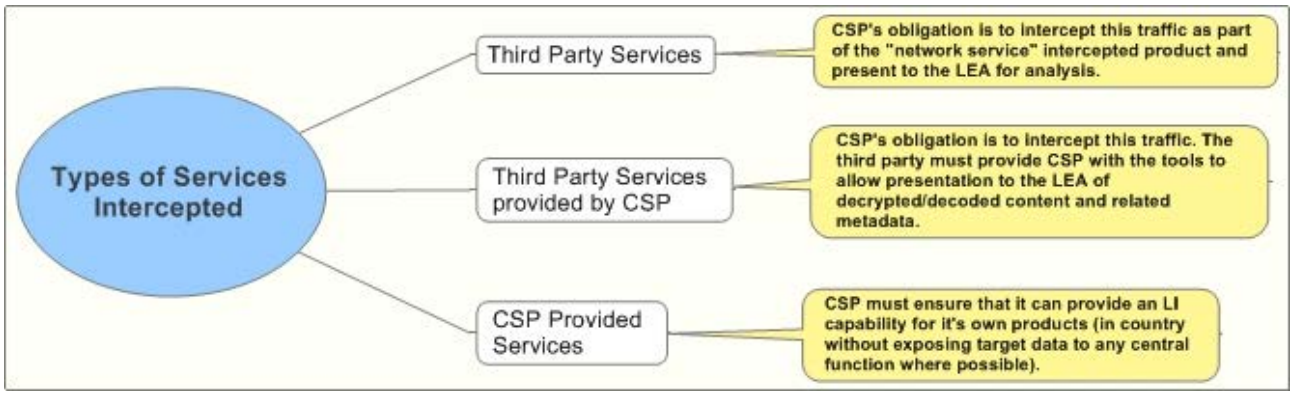


Figure 6-1: CSP LI Obligation According to Type of Service

6.3.2 Use of trusted third parties (TTP)

A CSP or LEA may choose to ask a TTP to help meet their obligations and needs. Based on agreements, the TTP may perform some functions in support of the responsibilities of the CSP and LEA. Ultimately, the responsibility to ensure the capabilities outlined in the present document are available, lies with the CSP or LEA.

6.4 LI implementation scenarios

Most existing LI solutions are either done per service or based on the type of access network, which is depicted in Figure 6-2.

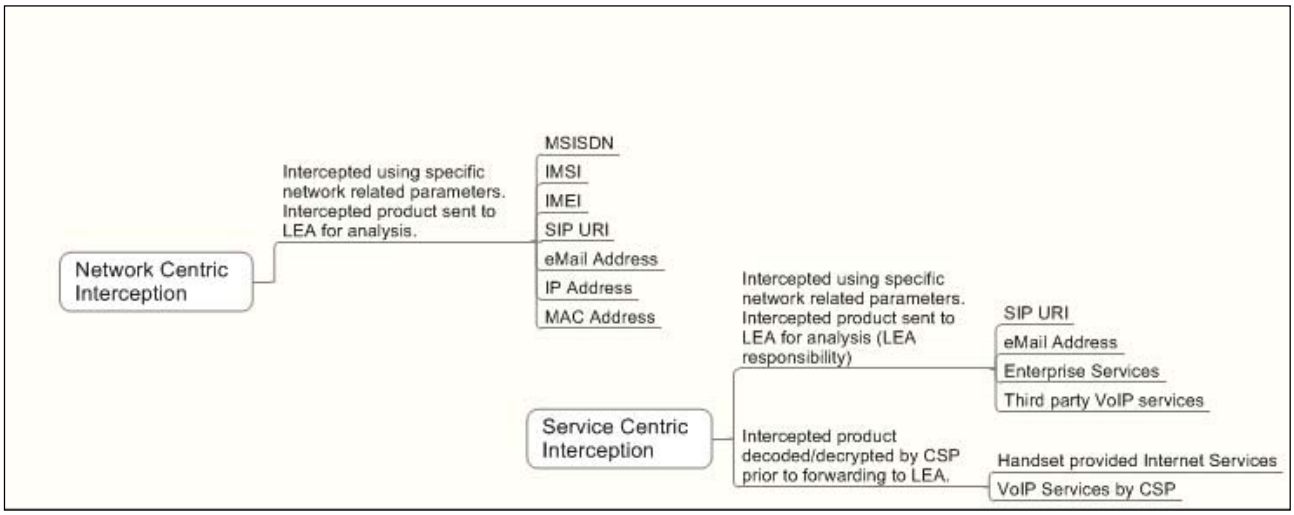


Figure 6-2: Types of Interception

Figure 6-2 also identifies some of the subject identities used in each type of Interception. Generically, these identifiers are either equipment based or service/subscriber based. In some existing LI solutions, LI can be accomplished on either known identifier, because the network or service provider is aware and maintains a binding between the two.

The ability to implement LI capabilities varies significantly among these groups as described in Figure 6-3. Thus, the expectations of LEAs are inherently constrained based on the access location and nature of the service provider and request-responses tailored to the type of provider.

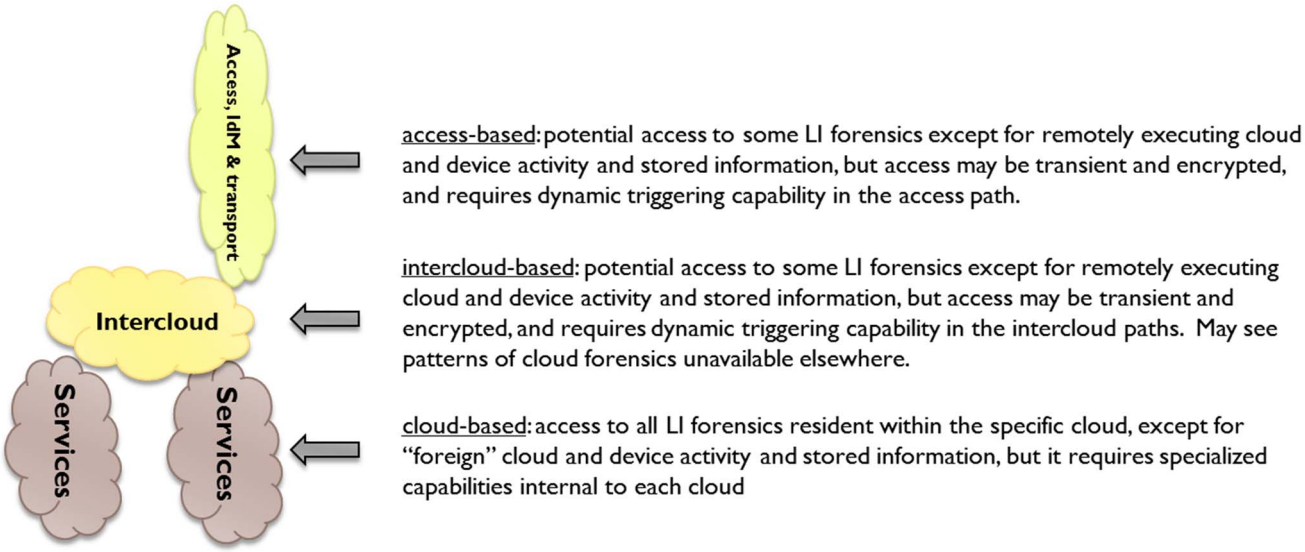


Figure 6-3: Cloud LI Implementation Scenarios

6.5 Implementation Challenges

6.5.1 Introduction

The introduction of Cloud services may increase the complexity and challenges for Lawful interception. The variations of Cloud services (e.g. IaaS, CaaS, PaaS) may introduce new or more complex business models and relationships amongst CSPs/C(L)SPs. Some specific challenges are described in more detail.

6.5.2 Encryption Challenge

Media and/or metadata may be encrypted by many parties.

Subscribers using Cloud services will expect C(L)SPs to protect/secure their data. This includes authenticating via secure connections and securely transferring data to/from their servers. It may also include encrypting "data at rest" when stored on the servers. In addition, subscribers of Cloud services may encrypt the data prior to transferring it "into the Cloud". End-user encryption usage may actually increase with Cloud services as this ensures a subscriber of exclusive control over their data and prevents C(L)SPs from accessing their subscriber's data for their own uses (e.g. data mining).

It is clear from ETSI TS 101 331 [i.1] that service providers who initiate encryption provide intercepted telecommunications (i.e. content and IRI) *en clair* (unencrypted) or if they cannot remove the encryption, provide the LEA with the keys and other information needed to access the information where such keys are available to the service provider. It is up to national regulations to determine how C(L)SPs need to meet the assistance obligations in ETSI TS 101 331 [i.1].

The "end-user encryption problem" exists in current (i.e. non-Cloud) networks today. Although Cloud Services may increase the problem for LEAs, it is not a new problem.

From ETSI GS NFV 001 [i.17]: the virtualized environment needs to guarantee complete isolation between users. Data encryption of cached content and link security is mandatory. The CSP/C(L)SP that employs network virtualization needs to meet the assistance obligations in ETSI TS 101 331 [i.1].

6.5.3 Multiple copies of intercepted traffic

The traffic may be intercepted in more than one location or on more than one CSP network.

6.5.4 Integration of Partial Communication Segments

The traffic intercepted from multiple communications as part of the same target session may need to be integrated.

6.5.5 Nomadicity

The ability for subscribers to change access technology (e.g. cellular, WiFi, DSL) and maintain continuity of some services exists today. If LI is at the service level, that service provider can provide the service logic, but may not have access to the communications content. If LI is at the access level, the access provider can provide what is being transmitted to and from that device, but since there is no understanding of the service(s) being used at the time, the access provider is unable to provide any assistance to the LEA on how to interpret the data. Neither the service provider nor the access provider may have the ability to assist the LEA with correlating identities across their domains. One of the challenges to this is that the identifiers used by the service provider and access network operator will be different and difficult for the LEA to maintain the binding of the identifiers/addresses between the domains.

By definition, Cloud services support a subscriber's nomadicity. The proliferation of smartphones and tablets coupled with a growing ubiquitous broadband network(s) are enabling people to stay constantly connected with an expectation of uninterrupted access to information. While subscribers own and use multiple devices for different purposes, smartphones with their smaller form factor are the primary devices for information and communications on the move.

A subscriber's ability to access their data and services from any device, especially devices with no known association (e.g. not owned) with the intercept subject, also exists today (e.g. Internet Cafes) and complicates an LEA's ability to initiate an access level lawful interception in a timely manner. The "any device, anywhere" characteristic of Cloud services just adds to the LEA's challenges.

6.5.6 Location

The location at which users are using Cloud based services may be difficult to discern in an assured manner.

While this clause uses ETSI TS 101 671 [i.2] as a basis for this discussion, it may be additionally valid for all other LI specifications.

ETSI TS 101 671 [i.2] defines Location information as "information relating to the geographic, physical or logical location of an identity relating to an interception subject." The HI2 interface port transports all Intercept Related Information (IRI), i.e. the information or data associated with the communication services of the target identity apparent to the network, which carries location information. From ETSI TS 101 671 [i.2] (V3.10.1):

```
Location ::= SEQUENCE
{
    e164-Number         [1] OCTET STRING (SIZE (1..25)) OPTIONAL,
        -- Coded in the same format as the ISUP location number (parameter field)
        -- of the ISUP (see EN 300 356 [5]).
    globalCellID        [2] OCTET STRING (SIZE (5..7)) OPTIONAL,
        -- See MAP format (see TS GSM 09.02 [32]).
    tetraLocation       [3] TetraLocation OPTIONAL,
        -- This optional parameter is not in use anymore, but is kept for backwards compatibility.
    rAI                 [4] OCTET STRING (SIZE (6)) OPTIONAL,
        -- The Routeing Area Identifier (RAI) in the current SGSN is coded in accordance with
        -- 3GPP TS 24.008 [41] without the Routing Area Identification IEI (only the
        -- last 6 octets are used).
    gsmLocation         [5] GSMLocation OPTIONAL,
    umtsLocation        [6] UMTSLocation OPTIONAL,
    sAI                 [7] OCTET STRING (SIZE (7)) OPTIONAL,
        -- format: PLMN-ID 3 octets (no. 1-3),
        -- LAC 2 octets (no. 4-5),
        -- SAC 2 octets (no. 6-7)
        -- (according to 3GPP TS 25.413 [82])
    ...,
    oldRAI              [8] OCTET STRING (SIZE (6)) OPTIONAL
        -- the "Routeing Area Identifier" in the old SGSN is coded in accordance with
        -- 3GPP TS 24.008 [41] without the Routing Area Identification IEI
        -- (only the last 6 octets are used).
        -- This parameter is duplicated from 3GPP TS 33.108 [61]
}
```

If a C(L)SP provides the services listed in clause 5.1.3, this location information definition may be insufficiently defined for a C(L)SP to provide meaningful information to the LEA. The C(L)SP may not know the target Cloud Service User's location or if known, it may not be able to provide the location information in the format defined. Since the location information is based on the underlying access technology (e.g. Tetra, GSM, UMTS), the CSP providing the target Cloud Service User access to the Cloud (i.e. Cloud Carrier per NIST SP 500-292 [i.22]), can provide the location information as defined in the existing parameter.

If location reporting is authorized for a specific service, the C(L)SP is obligated to report the location of the target Cloud Service User to the LEA. However, it is uncertain what information the C(L)SP has that relates to the "geographic, physical or logical location" of the target Cloud Service User.

The location information definition should be reviewed to determine if modification is needed to make it usable for a C(L)SP.

6.5.7 Target Identification

As mentioned in clause 5.4, the target of lawful interception may have several different network or service identities, depending on the network or service provider and type of interception being accomplished.

Each service provider, either CSP or C(L)SP, will have an ability to identify a particular subscriber or client. That identification may be one of the identifiers listed in Figure 5-2. It may also be a type of security credential or other identity management authentication.

Target identity(ies) may not traverse or be shared across different network or service providers. This may impact the ability of a service provider to isolate the target's communications to the exclusion of non-target communications.

A C(L)SP providing a conferencing service to a target of interception may provide service based on a log-in/password authentication while a CSP providing the target's mobile access to the network may use equipment identification in its authentication and authorization procedures. Neither service provider may be aware of the target's identity used in a network other than its own nor therefore, the binding between the two may not exist or be maintained. Dynamic Triggering may assist in the dynamic binding of target identities across network domains.

6.5.8 Correlation

Independent of interception type, LI solutions are comprised of Intercept Related Information (IRI) and Communication Content (CC). Correlation refers to the ability to associate the IRI with the CC. As stated in clause 5.4.2, different (or multiple) service providers may have access to the target's traffic. In the example in clause 5.4.6, the C(L)SP providing a conferencing service may have access to the IRI while the CSP providing the mobile network may have access to the CC. However, in this case, the mobile CSP may not be able to separate the conferencing CC.

6.5.9 Network Virtualization

LI needs on the network remain whether or not the network element is virtualized or not. As network functions are virtualized, operators and vendors need to ensure that the LI functionality is always available and that the integrity, correctness and security of LI information that crosses internal and external network interfaces are not adversely impacted.

6.6 Mobile Networks

6.6.1 Introduction

Network functions in mobile networks can also be virtualized. Use cases that address the 3GPP mobile network architecture can be found in ETSI GS NFV 001 [i.17].

Annex A provides a non-exhaustive list of use cases, to include those for Mobile Cloud Services. These use cases fall into four categories.

6.6.2 Non-MNO transited Cloud Applications/Services

Cloud applications or services that may not transit the MNO facilities (data in motion) are not considered in this clause.

Table 6-1: Use Cases where the Services do not transit an MNO

Clause	Use Case
A.3	VMI
A.4	VMI (Memory)
A.5	IPC
A.1	Telepresence
A.2	Telepresence (Externally hosted)
A.7	Mobile Portal/ Dash Board
A.8	VDI
A.9	Delayed VMI
A.10	File Sharing
A.17	File Sharing (7) SMB

6.6.3 Cloud Applications/Services integral to MNO

If the use cases provided are wholly within the MNO facilities, they fall within this category.

As this requires 3GPP to address the new features and service, which might reside in an MNO network, that further work is required and left for future work items.

Table 6-2: Use Cases where the Services are integral to MNO

Clause	Use Case	Comments
A.3	VMI	New services need to be defined in 3GPP SA1. New IAP functionally is required to support the feature. Should build on the present document.
A.4	VMI (Memory)	New services need to be defined in 3GPP SA1. New IAP functionally is required to support the feature. Should build on the present document.
A.5	IPC	New services need to be defined in 3GPP SA1. New IAP functionally is required to support the feature. Should build on the present document.
A.1	Telepresence	New services need to be defined in 3GPP New IAP functionally is required to support the feature.
A.6	Mobile Portal/ Dash Board	New services need to be defined in 3GPP. New IAP functionally is required to support the feature. Should build on the present document.
A.8	VDI	New services need to be defined in 3GPP. New IAP functionally is required to support the feature. Should build on the present document.
A.11	Delayed VMI	New services need to be defined in 3GPP SA1. New IAP functionally is required to support the feature. Should build on the present document.
A.10	File Sharing (1)	New services need to be defined in 3GPP SA1. New IAP functionally is required to support the feature. Should build on the present document.

6.6.4 Cloud Applications/Services Transit MNO via Proxies

Service that are proxied in the network may be handled in current systems, such as Session Border Controllers (SBC), Packet Data Gateways (PDG), backend Web services and may not require input from 3GPP. However existing Intercept Access Points (IAP) and collection and delivery functions may need augmentation to support these services:

- Location information reporting. When a user's device has simultaneous access over both Wi-Fi and the cellular networks, the network may receive location information from the PDG and the Mobile network. It is uncertain which location is reported or if both locations are reported.
- New IRI messages may be required.
- Different implementation and support via NNI to Cloud Servers.

Table 6-3: Use Cases where the Services transit MNO via Proxies

Clause	Use Case	Comments
A.11	File Share (2) Proxy	The services are only accessible while in the MNO network. New IAP functionally maybe required to support the feature. Service type/ IAP location to help LEA with composition of the application, decomposition of IRI messages, "Dirlist, file upload, down load, delete" (FTP type commands). Location if embedded in the application and available, associate decomposition, the identities used in the packet stream may not point to associates real identity, the identity of the resources, i.e. "documentname.doc".
A.14	File Share (4)	Access to the proxy is required to the public so others can access the files. This may require a new service to be defined in 3GPP. Current access from non 3GPP access is via the Packet Data Gateway (PDG). New IAP functionally maybe required to support the feature. Service type/ IAP location to help LEA with composition of the application, decomposition of IRI messages, "Dirlist, file upload, down load, delete" (FTP type commands). Location if embedded in the application and available, associate decomposition, the identities used in the packet stream may not point to associates real identity, the identity of the resources, i.e. "documentname.doc", the identity of the IP address associated with the session does not provide an identity of the session and the location of the user of the IP address.
A.15	File Share (5)	Public access to the proxy is required to the public so others can access the files. This may require a new service to be defined in 3GPP. Current access from non-3GPP access is via the PDG. New IAP functionally maybe required to support the feature. Service type/ IAP location to help LEA with composition of the application, decomposition of IRI messages, "Dirlist, file upload, down load, delete" (FTP type commands). The proxy may hide the identity of the user on the Cloud and if the Cloud is in the domain of the LEA, correlating information may be needed to examine evidence from the Cloud server. Time to Live parameters may be evidential. Access attempts to a target users files, identifying information. Multiple simultaneous open sessions to the same account and files, identifying information (each device may have an ID).
A.16	File Share (6)	Access to the proxy is required to the public so others can access the files. This may require a new service to be defined in 3GPP. Current access from non 3GPP access is via the PDG. Access to encrypted services may already be covered with Media Security services. New IAP functionally maybe required to support the feature. Service type/ IAP location to help LEA with composition of the application decomposition of IRI messages, "Dirlist, file upload, down load, delete" (FTP type commands), the proxy may hide the identity of the user on the Cloud and if the Cloud is in the domain of the LEA, correlating information may be needed to examine evidence from the Cloud server. Time to Live parameters may be evidential. Access attempts to a target users files, identifying information. Multiple simultaneous open sessions to the same account and files, identifying information (each device may have an ID).
A.18	File Share (8)	In this use case, the target and his files are associated to a MNO proxy server and all request to access files and association to the file are passed to the MNO to manage. New IAP functionally maybe required supporting the feature. Service type/ IAP location to help LEA with composition of the application decomposition of IRI messages, "Dirlist, file upload, down load, delete" (FTP type commands), the proxy may hide the identity of the user on the Cloud and if the Cloud is in the domain of the LEA, correlating information may be needed to examine evidence from the Cloud server. Time to Live parameters may be evidential. Access attempts to a target users files, identifying information. Multiple simultaneous open sessions to the same account and files, identifying information (each device may have an ID).

6.6.5 Cloud Applications/Services Transit MNO via Policies

Services that have policies flow, can provide the same functionality as described in the proxies scenarios, however they requires support for:

- Location information reporting. When a user's device has simultaneous access over both Wi-Fi and the cellular networks, the network may receive location information from the PDG and the Mobile network. It is uncertain which location is reported or if both locations are reported.
- New IRI messages may be required.

Table 6-4: Use Cases where the Services are forced to transit MNO via Policies

Clause	Use Case	Comments
A.12	File Share (3)	The use of FQDN in ANDSF to keep all services within the MNO facilities or directed to IAP.
A.19	ANDSF	The MNO decides which services and IP flows need to flow back into its core network. Only the Services it supplies are routed back, basic Web browsing may not be routed home while on a hotspot New IAP functionally maybe required to support the feature.

6.7 Mobile Networks

6.7.1 General

This clause derives needs from the Use Cases for Operators to deploy Branded Mobile Cloud Solutions that meet the various regional regulatory lawful access obligations. This clause only deals with those cases that transit MNO facilities as identified in clause 5.5.

In general not all regulatory domains have the same lawful access obligations. The present document will assume the most stringent needs such that any specification created or modified will support the requirements, while regional implementation can deal with the capability in regional variations or optional parameter settings. It has to be noted that if a new field or parameter in ETSI TS 133 107 [i.12] is needed, ETSI TS 133 108 [i.19], then it is mandatory that it is to be included in the specification. However the delivery of the information to LEA may be optional depending on the regional differences.

6.7.2 Mobile Cloud

Lawful access obligations vary by national regulations, but generally include interception of private communications, disclosure and retention of an operator's subscriber information and their services. These needs are described in national laws and regulations and also define the instruments required to invoke access. Other regulation may define the qualification of a Communications Service Provider (CSP).

Each of these aspects of lawful access has different technical needs. The derived needs in the present document should be viewed only in terms of interception or data in motion across a 3GPP network as outlined in ETSI TS 133 106 [i.11]. Granted, some or all the needs may be used by other systems that support retention and or disclosure or are subject to search and seizure.

The definition of a "Subject of investigation" may vary by national regulation and may evolve over time. A Subject's service may be any communication, feature or function that operates on behalf of the Subject even if the Subject is not presently communicating with the service, examples, email, voice mail and Cloud services like file sharing.

6.7.3 General

ETSI TS 133 106 [i.11] describes the obligations of LEA's for mobile networks. The following list is derived after some analysis in the use cases from annex A.

[R001] MNO provided Cloud services (White labelled or in house) require lawful access.

[R002] Lawful access may extend to MNO services that transgress the operator domain (non 3GPP access Domains).

[R003] Lawful access occurs in the regulatory Domain of the MNO.

[R004] Lawful access may occur in the regulatory domain of the Cloud Service if supported and authorized.

[R005] MNO provided Cloud service provides the capability to provide IRI and Content related intercepts.

[R006] MNO is required to assist the LEA to provide content in the clear of a provided Cloud service.

[R007] Lawful access is not detectable by the subject and or the subject services or others users.

[R008] Lawful access reports the location.

[R009] Lawful access reports all identities used by the subject.

[R010] Lawful access reports access to the subject's Cloud service by others.

[R011] A Cloud service identifier should be available to aid collection systems.

NOTE: If there are multiple Cloud services and vendors providing different services for the MNO, an identifier may assist LEA in future investigate work. Disclosure from the MNO may not identify uniquely the Cloud service. Retention services might be able to determine the Cloud Services and end points (the IP address may not be static or may change due to DNS query and cache location of servers) If there are multiple proxies used as outline in [R017] the identifier might assist in future search and seizure activities.

6.7.4 Proxy

[R012] Session timers (Time to Live) should be set to allow proxy systems to be able transpose address.

NOTE 1: Concerns could arise whether changing the messages results in contamination of evidence and if S or CSCF do this anyway as B2B user agents, clarification may be required. Also note that the user may never get the file and there may never be a retry. The service may not indicate the failure so the LEA may have the file and the user may not, if the proxy requests the file as per use case located in annex A.

[R013] Any hashes used by the Cloud service should be known to the proxy, such that reconstructed addresses can be created without errors.

[R014] If the proxy and Cloud client report non 3GPP access parameters, they should be provided as IRI.

[R015] The proxy reports the IP addresses used by the subject.

[R016] The proxy is uniquely identified in lawful access messages.

[R017] The network should allow multiple proxies to be deployed in a MNO network, allowing redundancy and reducing latency.

NOTE 2: Data retention is not addressed, additionally a proxy may request copies of files in separate messages if the content is delivered from the Cloud service directly from the CSP and not through the proxy.

6.7.5 ANDSF

[R018] It should be possible to configure policies for subjects on the fly to restrict Cloud and MNO base services to be kept with the MNO network.

[R019] The change in policies should be undetectable by the subject or the subject services.

[R020] The IP addressed used for non-3GPP access is captured.

[R021] The ANDSF client should report additional information such as SSID, Local IP address.

NOTE: The ANDSF client or client server may have additional information in regards to the user location as policies are used to steer traffic to particular Wi-Fi access networks, including SSID.

7 Traditional LI models and methods applied to the Cloud environment

7.1 Introduction

As described in clause 5, network virtualization and Cloud services of existing telecommunications services for which there are LI handover specifications can generally use those specifications and associated models to meet handover obligations. This clause describes those specifications and how they can be adapted to the Cloud environment, together with extensions to the models that can be used for newer services.

7.2 Traditional LI models

The diagrams of annex E (informative) of ETSI TS 101 331 [i.1] may provide a conceptual foundation for Cloud services LI.

LI models for telecommunications services are currently found in:

- ETSI TS 101 671, "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic [i.2];
- ETSI TS 102 232-2: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 2: Service-specific details for Messaging services" [i.4];
- ETSI TS 102 232-3: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 3: Service-specific details for internet access services" [i.5];
- ETSI TS 102 232-4: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 4: Service-specific details for Layer 2 services" [i.6];
- ETSI TS 102 232-5: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 5: Service-specific details for IP Multimedia services" [i.7].

The standard handover interface developed by TC LI for LEA/CSP use is depicted in Figure 7-1.

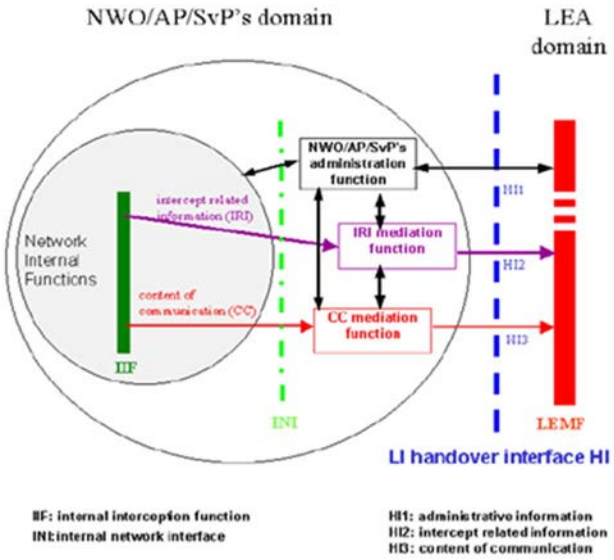


Figure 7-1: Standard CSP-LEA interface for traditional services

7.3 Adaptation to the Cloud environment

Irrespective of how the services are provided, obligations for LEA necessitate the interception of designated traffic in a secure and trusted manner sufficient to meet any applicable judicial evidence obligations, as expeditiously as possible. Examples are depicted in Figure 7-2.

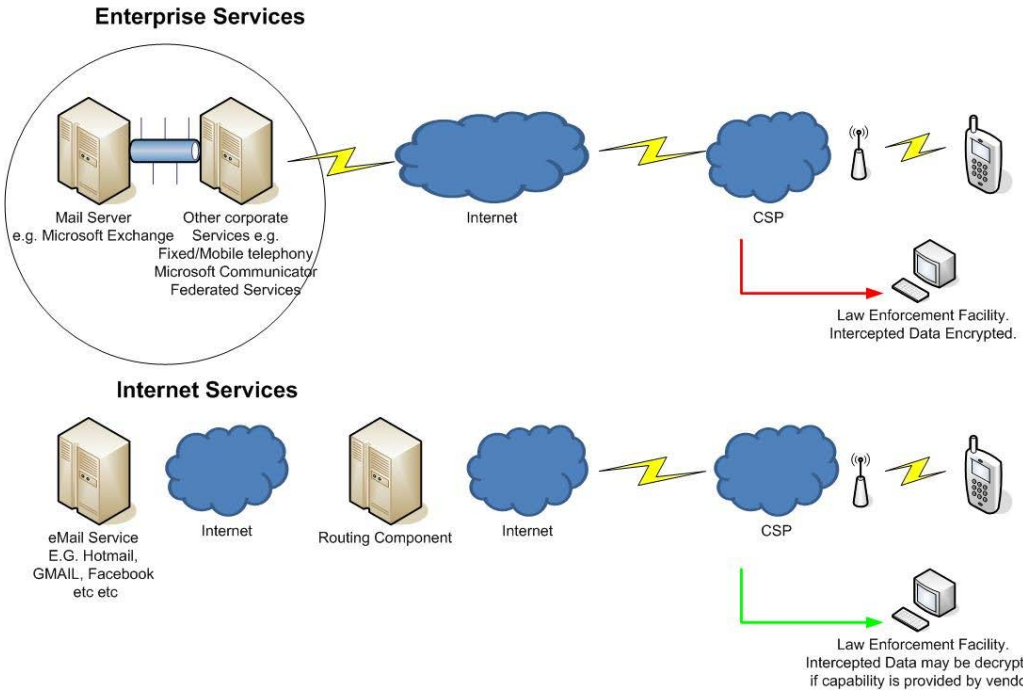


Figure 7-2: Adaptation of LI to the Cloud Environment

7.4 Handover Interfaces for new Cloud services

The basic request-response interface demarcation between the LEA and CSP will continue to exist. However, what gets transferred across that interface is likely to be fundamentally different. Applications, services and the available information expected to be returned by the C (L) SP are generally very different in the new Cloud services described in clause 5.

There are no existing specifications for describing and structuring Cloud targets, applications and available LI response information.

7.5 Handover interfaces for virtualized network elements

Handover interfaces between the LEA and CSP will continue to exist.

7.6 Hybrid Services

7.6.1 Introduction

Hybrid Cloud services are a composition of two or more clouds (private, community or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g. Cloud bursting for load-balancing between clouds).

7.6.2 Volte

Given the options in how certain network elements can be deployed and how they may be geographically shared it is possible that a combination of traditional telecommunications and Cloud LI techniques may be required e.g. centralized HSS or TAS.

7.6.3 Peer to Peer Services

Some peer to peer services only contact a centralized point to ensure they know what IP address to use to contact another user - the media is not routed via any easily predictable infrastructure. However this setup information may, if structured correctly and unencrypted allow the various CSPs intercept the traffic. See Figure 7-3.

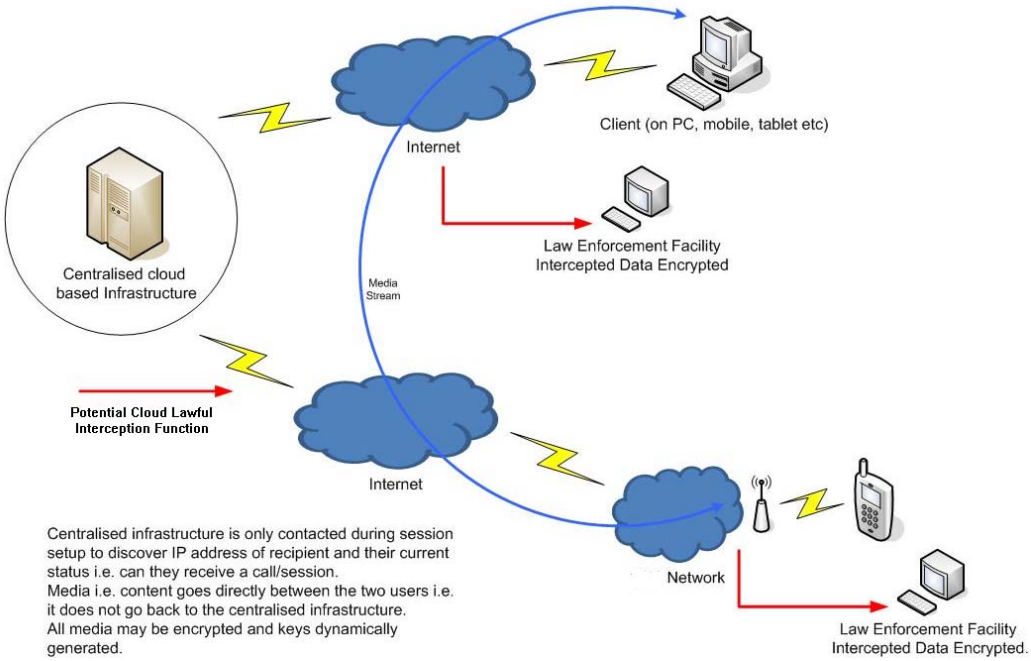


Figure 7-3: Peer to Peer call/session flow

7.7 Cloud Lawful Interception Function (CLIF)

In order to maintain LI production capabilities, a C (L) SP can implement a Cloud Lawful Interception Function (CLIF).

Table 7-1 describes CLIF use cases to accommodate implementation challenges.

Table 7-1: Cloud Lawful Interception Function Use Cases

Locations	Cloud Lawful Interception Function
Cloud based provider outside LEA jurisdiction, but service is made available within jurisdiction	CLIF is required to enable the C(L)SP to intercept the traffic
Cloud based provider within the LEA jurisdiction with service carried internally	Although the LEA may be able to force the Cloud service provider to intercept within its own infrastructure, it may be better to also use the a CLIF - thus maintaining standard interfaces, capabilities and coverage

8 Security of LI in a Cloud or Network Virtualized environment

8.1 Lawful Interception security

Existing LI specifications include extensive security capabilities. See Handover specification for IP delivery, ETSI TS 102 232-1 [i.3]. Some comparable secure delivery capability is necessary for the Cloud service environment - not only for delivery, but for requests such as warrants described in ETSI TR 103 690 [i.8].

Additional LI security capabilities may also need to be specified relating to avoidance of detection and compartmentalization of LI implementations in Cloud services environments.

National regulations may identify specific security practices and needs. Generally, LI mechanisms, capabilities and operations are provided protection from disclosure to unauthorized personnel (e.g. the target, other subscribers, CSP employees not involved in LI activities). LI activities should be accomplished in an undetectable manner. CSPs develop security practices and procedures. Handover of intercepted product is typically done in a secure, reliable manner, utilizing encryption or secure transfer protocols, to ensure data integrity.

8.2 Cloud services security

C (L) SPs ensure that their infrastructure is secure and that client data and applications are protected. This is done through security controls to prevent attacks and mitigate vulnerabilities, detect attacks and reduce data/resource loss and damage in the event of an attack or security compromise.

C (L) SPs will need to manage access control for client information and computing resources, restricting unauthorized access. Private or sensitive data may require additional security. Digital identities and credentials are protected. Aggregation of customer data or activity produced may also require additional protection.

C (L) SPs and their customers may have to compliance with national laws concerning various issues such as contracts, e-discovery, privacy or stored and personal information (e.g. credit cards, health information). These may require maintaining logs and audit trails, which themselves may require additional security.

For purposes of the present document, Cloud services security consists of capabilities that enable the assessment and mitigation of risks associated with those services and the supporting infrastructures. Security capabilities of interest for Lawful Interception purposes generally encompass either Identity Management or security related implementations that enable or facilitate acquisition of traffic or patterns of interest.

The Cloud security work is spread across many of the forums identified in annex B and constantly evolving.

In regards to the Cloud legal aspects, it is to be expected that many Cloud computing scenarios will span the laws of multiple jurisdictions that may all potentially apply.

The same data may be processed in multiple jurisdictions at the same time and the actual location of a user's data may be difficult to determine.

The combinatorial character of the mobile Cloud services, across multiple resource domains, infrastructure domains, security domains and jurisdictions domains, makes the task of developing LI solutions for Cloud services particularly challenging.

The market opportunities of the mobile Cloud services might be impeded, for the 3GPP mobile operators, by some conditions of their operating licenses, like the regulatory obligations for LI that are an intrinsic part of any operational license.

Even if not specifically spelled out for Cloud services cases, as the mobile operator domain is a component of the combination of domains that contributes to the feasibility and delivery of the Cloud services, the LI obligations are most likely to be implicitly extended by the regulators to Cloud services.

8.3 Security Considerations in a Virtualized Network Environment

A CSP or C (L) SP may implement network virtualization within their own architecture or may outsource portions of their virtual network to other providers. In either case, the security needs to protect LI capabilities and operations remain the same, independent of any level of virtualization.

9 LI - Cloud gaps and challenges

9.1 Generic Cloud LI interface specification gap

The present document is intended to provide an initial overview of Cloud LI, to include mobile operators that provide white labelled or Branded Mobile Cloud Services. Challenges to support lawful access of services are identified and discussed. The present document focuses on Interception of data in motion and any missing elements from current Specifications.

The use cases in annex A were analysed and from these non-exhaustive lists of use cases three scenarios emerged:

- Scenario 1: Cloud Services not transiting the network or remain wholly within the network's facilities,
- Scenario 2: Cloud Services that transit the network facilities via proxy,
- Scenario 3: Cloud Services that transit the network facilities via policies.

In Scenario 1, these services should be supported by ETSI and any LI documents generated from the present document. Integration or aspects of functions required with ETSI TS 133 106 [i.11], ETSI TS 133 107 [i.12], ETSI TS 133 108 [i.19] are beyond the scope of the present document.

If it is determined that new work is needed, the following should be considered:

a) How location, Cloud application identity, IMS interaction are reported for those services supported.

b) If the Mobile Cloud service is in a different Regulatory Domain and supports ETSI and is supported through mutual legal assistance instruments.

c) If the Mobile Cloud service is in a different Regulatory Domain and supports ETSI LI Cloud collection and is supported through mutual legal assistance instruments and supports dynamic triggering.

d) Incorporation of any Derived Obligations from clause 5.

However, there remains an important obvious need for a specification that establishes a generic interface for Cloud services. Large data centres are expanding worldwide and transforming the service provisioning globally. Components of that environment, such as "application"-based services, complicate the challenges.

Considering this significant exponential scaling of Cloud service environment, generic specification between C (L) SPs, CSPs and LEAs is essential for all parties. It should include a structured trusted means to request LI capabilities and receive a response as well as best practices for implementations. The Cloud LI Function identified in clauses 5 and 6, above, represents a common, generic, infrastructure-based approach.

9.2 Specific Cloud LI specification gaps

9.2.1 General

Scenarios 2 and 3 may require additional specification(s) or CSP/C (L) SPs may benefit from a best practices or implementation guide.

9.2.2 Scenario 2: Cloud Services that transit the network facilities via Proxy

It is left to implementation how a mobile operator will meet their lawful access obligations. The present document illustrates several examples in the Use Cases that may be used. The Uses Case where not exhaustive and there may be other implementations. However from the list provided the following issues were noted:

a) Location information reporting. When a user's device has simultaneous access over both Wi-Fi and the cellular networks, the network may receive location information from the PDG and the Mobile network. It is uncertain which location is reported or if both locations are reported.

b) New IRI messages may be required.

9.2.3 Scenario 3: Cloud Services that transit the network facilities via Policies

With the introduction of access Network Discovery and Selection Function (ANDSF) it is possible for an MNO to specify which application is routed through the MNO network while accessing hotspots or other Wi-Fi/IP networks. Work is still progressing in this area. However from the list provided the following issues were noted:

a) Location information reporting. When a user's device has simultaneous access over both Wi-Fi and the cellular networks, the network may receive location information from the PDG and the Mobile network. It is uncertain which location is reported or if both locations are reported.

b) If new IRI messages are required for some Cloud Services.

c) Whether a Subject and or the Subject's Cloud Service can detect invocation of lawful access.

9.2.4 Target Identity expressions for Cloud LI

Unlike the traditional telecommunications and Internet environments, target identities, in a Cloud environment are unlikely to be well structured and are frequently temporary. With more than two million applications and other Cloud services and expansion rates of 10 % per month, the identities of targets may vary significantly. Indeed, in some Cloud services, a target identity may consist only of a set of attributes that collectively can be associated with a specific individual.

There is a compelling need to develop an extensible structured expression for a "virtual target identity" that enables law enforcement and CSPs/C(L)SPs to effectively describe a target in a Cloud environments. This should expand how target identities are currently defined. Without such a structured expression, it is not possible to describe the desired target and every request becomes a "free form" text description that is difficult and costly to produce and implement.

9.2.5 Application Identity expressions for Cloud LI

Similar to the virtual target identity challenge/gap described above, in a Cloud environment, the applications number in the hundreds of thousands and are constantly changing. Some applications may also be malware.

A number of organizations and vendors are attempting to develop means for instantiating virtual service application identities in conjunction with traffic management, cybersecurity and LI. Even more advanced in the area of application identities is the structure expression work progressed by US government agencies for describing malware known as the Malware Attribute Enumeration and Characterization (MAEC). This language specification is also scheduled to be adopted by the ITU-T as Recommendation ITU-T X.1546 [i.18].

There is a compelling need to develop an extensible structured expression for a "virtual application identity" that enables law enforcement to effectively describe an application in a Cloud environment. Without such a structured expression, it is not possible to describe the service application associated with the target and every request becomes a "free form" text description that is difficult and costly to produce and implement. A new work item to produce this specification seems appropriate.

9.2.6 Virtual Observable (VO) expressions for Cloud LI

In a Cloud environment, available information, whether LI content or IRI associated with the virtual target identity, is usually very diverse, associated with applications that are not well understood or acquired from many kinds of distributed network resources. The information of interest may also include complex resource use signatures within the virtualization environment.

One of the significant emerging means for capturing and exchanging this information is the creation of a common modular structured specification for "observables" known as Cyber Observable eXpression (CybOX™). It can form the basis for TC LI work for a Virtual Observable expression for Cloud LI.

NOTE: From: http://cybox.mitre.org/about/faqs.html#A1: CybOX™ is a standardized language for representing cyber observables, whether from observation in the operational cyber domain or as patterns of observables that could be observed. Cyber observables are events or stateful properties that occur or may occur, in the operational cyber domain, such as the value of a registry key, deletion of a file or the receipt of an http GET.

There is a compelling need to develop an extensible structured expression for "virtual observables" that enables the acquisition and handover of information in a Cloud environment. Without such a structured expression, it is not possible for a C(L)SP or CSP to respond to a LEA request with information associated with the target. Every response becomes a "free form" text description that is difficult and costly to process by LEAs.

9.2.7 CLIF Specifications

In relatively static, traditional network environments, a common set of handover interface (HI) specifications for receiving and responding to structured expressions for LEA Lawful Interception production requests have been widely used over many years. Additionally, an Intercept Access Point is necessary to provide coverage for the services to be intercepted. However, in a Cloud-NFV environment, the equivalent capabilities will likely be scattered across many different physical and virtual infrastructures - under the control of diverse users and providers, as well as subject to different legal jurisdictions. The associated resources are frequently transient and may not have loci specified by traditional network-based identifiers. The development of CLIF specifications is essential to maintaining LEA LI obligations.

10 LI - Network Virtualization gaps and challenges

In NFV, exact physical deployment of a VNF instance on the infrastructure is not visible from the end-to-end service perspective, with the exception of guaranteeing specific policy constraints. VNF instances and their supporting infrastructure need to be visible for configuration, diagnostic and troubleshooting purposes ETSI GS NFV 002 [i.13].

Some areas to be analysed include when network functions are virtualized:

- The need to identify and report service instance(s).
- If network node (i.e. IAPs/ICEs) identities are affected.
- If additional LI functionality is needed in the NFV Management and Orchestration functions.

11 Conclusions and Recommendations

Major gaps and challenges exist that are increasingly larger with respect to enabling law enforcement to request and receive Cloud/virtualization information. The gaps go substantially beyond Cloud/virtualization networks and services. Traditional LI approaches in dedicated service architectures like telephony are largely irrelevant in a world involving multiple service providers, as well as unknown and constantly changing architectures, applications and devices.

Service and network architectures are non-monolithic, with multiple operators involved in supplying a service to a single user. It is not unusual for the service provider at the application/signalling layer to be different from the access provider. In addition, for some services it is necessary to have the option to perform interception in the core network where there is not always a link between the identifiers used in the application layer and the identifiers used in the access / transport domain (generally IP Address).

Cloud/virtualization implementations with a large number of constantly moving smart phones, tablets and similar devices using diverse and distributed applications and related services, take the challenges to a whole new level. It is essential to develop new future-proof, infrastructure-agnostic means for law enforcement to specify the acquisition of available real-time case intelligence information from diverse information sources using actor-specific application patterns and correlate that information. At the same time, these means allow for considerable flexibility among service, Cloud and network providers, vendors and trusted third parties in determining exactly how they will comply with an LI order from government authority within their facilities.

The cyber threat intelligence community is also facing an almost identical challenge in the acquisition, integration and exchange of real-time attack information. That community provides structured information exchange approaches that also meet law enforcement needs. By leveraging the cyber threat intelligence community platforms, the law enforcement community can enhance its own capabilities with this major development activity and reduce redundancies or disparate approaches.

Annex A:
Several Use cases

A.1 Telepresence use case 1: TSP offers Telepresence and all participants are subscribers of the TSP

a) Overview

1) This use case describes basic telepresence service. A TSP offers Telepresence and all the participants are subscribers to that TSP.

b) Actors

1) The users are Jean (the subject of the lawful interception) and her two associates: Greg and Peter.

2) McCloud is the mobile TSP/Cloud service provider providing a Telepresence Service.

3) The Alleghany County Police department is the LEA authorized to perform the electronic surveillance.

c) Preconditions

1) Jean, Greg and Peter all are subscribers of the McCloud Telepresence services.

2) The Alleghany County Police Department as obtained the lawful authorization to perform electronic surveillance on Jean, who is suspected of involvement with some illegal activity.

3) The Alleghany County Police Department has provided McCloud with this lawful authorization for assistance in intercepting Jean's communications, which includes use of McCloud's Telepresence service.

4) McCloud is able to deliver intercepted communications of its Telepresence Service to authorized LEAs.

5) Jean, Greg and Peter all are using UEs which are active on the McCloud network. However, each has different video display capabilities.

d) Actions

1) Jean initiates Telepresence (conference) session with Greg and Peter.

2) Jean, not having extensive video administration experience, relies heavily on the McCloud Help Desk Service for assistance in using the service (e.g. to initiate and troubleshoot problems) while Peter and Greg join her in the Telepresence meeting.

3) Peter and Greg accept the invitation to join the Telepresence session and are added to the conference.

4) The McCloud surveillance facilities identify that a target of LI has initiated communication covered by the LI authorization and begins delivery of the communication to the LEA.

5) The Alleghany County Police Department begins receiving Jean's intercepted communications (i.e. IRI and CC for all required services as identified in the lawful authorization). The IRI and CC for the Telepresence service is delivered separately and the CC is the media that is sent to/from Jean (the Subject).

6) Jean, Peter and Greg discuss criminal activities they are planning, showing maps and pictures of the criminal venue (e.g. bank and surrounding streets for their "get-away"). Greg shows a short silent movie clip of the bank guards to show their routine and guard positions.

7) McCloud's Telepresence Service adapts the video delivery to each UE based on the UE capabilities and for network optimization.

8) Peter's UE display is small and he is unable to see the important details of the video that Greg is sharing, since he is unable to zoom in for a closer view.

9) The Telepresence session ends.

e) Results

1) Jean, Grep and Peter have finalized their plans for illegal activity and were unaware that any LI had occurred.

2) The Alleghany County Police Department received the IRI and CC of Jean's communications. Using that information in their investigations, they prevent a crime from occurring.

3) Met their regulatory obligation to unobtrusively deliver communication to the authorized LEA.

f) LI Discussion/Challenges

1) McCloud has a legal obligation to provide LI for the Telepresence session. Whether the video is provided to Law Enforcement is a national option. At a minimum, the audio of this conference, as well as the IRI is required to be reported, as Telepresence is a conference per 3GPP definition. The exact set of events and information is outside the scope of this use case (as SA3-LI has not yet discussed/agreed/defined LI for Telepresence).

2) The identities of the participants are known to McCloud, as they are all subscribers to McCloud's Telepresence service. The McCloud Telepresence Service has the service logic for Jean's Telepresence session, the identities of the participants and access to the media.

3) As with any other service lawfully intercepted, if McCloud provides encryption for the Telepresence Service, McCloud is responsible for either decrypting or providing the keys to law enforcement to decrypt.

A.2 Telepresence use case 2: Telepresence is offered by a Third Party provider. Participants are subscribers of the same or different TSP(s)

a) Overview

1) This use case describes basic telepresence service. The mobile TSP acts as a "Cloud carrier" for the Cloud provider's Telepresence service.

b) Actors

1) The users are Jean (the subject of the lawful interception) and her two associates: Gabor and Terry.

2) McCloud is the mobile TSP/Cloud carrier. Jean and Terry are subscribers of McCloud.

3) McCloud provides Jean with mobile broadband and voice services.

4) ExcellAlex Mobile is a mobile TSP. Gabor is a subscriber of ExcellAlex Mobile.

5) TellyServ is a (third party) Cloud service provider providing the Telepresence Service. TellyServ is NOT offering Telepresence Service on McCloud's behalf nor does TellyServ have any business relationship with McCloud.

6) Jean, Terry and Gavor all subscribe to TellySErv's Telepresence Service.

7) The Maryland State Police do not provide ExcellAlex Mobile a lawful authorization as it is not providing a service to Jean (the Subject).

c) Preconditions

1) The Maryland State Police has obtained legal authority to perform electronic surveillance on Jean, who is suspected of involvement in illegal activity.

2) The Maryland State Police has provided McCloud and TellyServ with this lawful authorization for assistance in intercepting Jean's communications.

3) McCloud and TellyServ both are able to deliver intercepted communications to authorized LEAs.

4) The Maryland State Police do not provide ExcellAlex Mobile a lawful authorization as it is not providing a service to Jean (the Subject).

5) Jean and Terry are using UEs that are active on the McCloud network. Gabor is using a UE that is active on ExcellAlex Mobile. All three UEs (Jean's, Terry's and Gabor's) are active with TellyServ to use the Telepresence Service.

d) Actions

1) Jean initiates a Telepresence (conference) session with Gabor and Terry.

2) Jean, not having extensive video administration experience, relies heavily on the TellyServ's Help Desk Service for assistance in using the service (e.g. to set-up the meeting and troubleshoot problems) while Gabor and Terry join her in the Telepresence meeting.

3) Terry and Gabor accept Jean's invitation to join the Telepresence session and are added to the conference.

4) McCloud surveillance functions identify that a target of LI has initiated a communication covered by their lawful authorization (i.e. broadband data access, SMS and VoIP) and begin delivery of the communications to the LEA. Note some of the TellyServ Telepresence is delivered as part of the McCloud's mobile broadband intercepted communications.

5) TellyServ surveillance functions identify that a target of LI has initiated a communication covered by their lawful authorization (i.e. Telepresence) and begin delivery of the communications to the LEA.

6) The Maryland State Police begin receiving Jean's intercepted communications (i.e. IRI and CC) from both McCloud and TellyServ.

7) Jean, Terry and Gabor discuss criminal activities, showing maps and pictures of the criminal venue (e.g. bank and surrounding streets for their "get-away"). Gabor shows a short silent movie clip of the bank guards to show their routine and guard positions.

8) The telepresence session ends.

e) Results

1) Jean, Terry and Gavor finalized their plans for illegal activity and were unaware that any LI had occurred.

2) Jean was also unaware of the LI on her broadband access.

3) The Maryland State Police received the IRI and CC of Jean's communications. Using that information in their investigations, they prevent a crime from occurring.

4) McCloud met their regulatory obligation to unobtrusively deliver intercepted communications to the authorized LEA.

5) TellyServ met their regulatory obligation to unobtrusively deliver intercepted communications to the authorized LEA.

f) LI Discussion/Challenges

1) McCloud has a legal obligation to provide LI for the services that they offer the target. In this use case, they do not offer the Telepresence Service, so they are not obligated to provide separate delivery of this service. Since it is "available" in Jean's packet data stream, it is delivered as part of McCloud's packet data interception. McCloud isolates and reports Jean's intercepted voice, SMS and packet data/broadband services per their LI solutions. McCloud uses the identifiers that are available in their services and network.

2) TellyServ has the legal obligation to provide LI for the services that they offer the target. In this use case, this is only the Telepresence Service. They provide the CII and CC for the Telepresence service per their LI solution and suing the identifiers that are used in the Telepresence Service. TellyServ knows the identities of the participants; they have the service logic and access the media.

3) As with any other service lawfully intercepted, if TellyServ provides encryption for the Telepresence Service, TellyServ is responsible for either decrypting or providing the keys to law enforcement to decrypt.

A.3 Virtual Machine Image (VMI) Basic Use Case

a) Overview

1) This use case describes basic VMI operation when the image is explicitly created by the user.

b) Actors

1) The user is John.

2) McCloud is the Cloud service provider providing IaaS on a variety of target hardware platforms but a single hypervisor (VMM).

c) Preconditions

1) John is a subscriber of the McCloud services and has VMI management privileges for private, shared and public images.

2) John begins with a public VMI with LINUX OS in initialized state.

d) Actions

1) John selects a public VMI which has LINUX and appropriate application libraries initialized to run on a specific target machine type.

2) John installs and initializes an application which manages his illegal activity.

3) John then initiates a VM snapshot to save the VM state as a new shared VMI.

4) John's cohorts are then able to logon to the new VM under the standard LINUX login services that John manages.

5) John also distributes the VMI name for other groups engaged in illegal activity to also use.

e) Results

1) There is a VM environment operating under John's control supporting the purposes of the illegal activity.

2) The VMI which is tailored for illegal activity is available for other groups to also support other illegal activity.

f) Challenges for interception

1) The VMI is hardware and VMM specific. The target hardware platform may be Cloud service provider specific.

2) The identities of the users of the VM may not be known to the Cloud service provider since the user identity management on the VM is by the system administrator of the hosted OS.

3) The identities of the VMIs are Cloud service provider, VMM specific.

4) Identifying the target OS may not be known by the Cloud service provider, but require parsing the VMI.

5) Identifying relevant data may require reverse engineering the application since the source code may not be available and then parsing the VMI.

A.4 In Memory File System or Database

a) Overview

1) This use case describes basic VMI operation when the file system or database of interest is in the main memory of the VM as opposed to residing on a structured mass storage element.

b) Actors

1) The user is John.

2) McCloud is the Cloud service provider providing IaaS or PaaS on a variety of target hardware platforms but a single hypervisor (VMM).

c) Preconditions

1) John is a subscriber of the McCloud services and has installed an in memory file system and database system on the OS running in the selected VM.

d) Actions

1) John activates the VMI with the in memory file and database systems/

2) John installs and initializes an application which manages his illegal activity.

3) John's cohorts are then able to logon to the new VM under the standard LINUX login services that John manages.

e) Results

1) All of the state (data) of the illegal activity are contained within the VM image or the active VM.

f) Challenges for interception

1) The VMI is hardware and VMM specific. The target hardware platform may be Cloud service provider specific.

2) The identities of the users of the VM may not be known to the Cloud service provider since the user identity management on the VM is by the system administrator of the hosted OS.

3) Identifying the target OS may not be known by the Cloud service provider, but require parsing the VMI.

4) Identifying relevant data may require reverse engineering the application since the source code may not be available, parsing the file and database systems and then parsing the VMI.

5) The VMI created by the user or the latest VMI created for user triggered check pointing, may not contain the most current data of interest. Rather that it exists in the active VM.

A.5 Distributed Application Communicating through IPC

a) Overview

1) This use case describes an application which is distributed across multiple VMs hosted by the same Cloud service provider. The distributed parts of the application communicate through an Inter Process Communication (IPC) service.

b) Actors

1) The user is John.

2) McCloud is the Cloud service provider providing IaaS or PaaS on a variety of target hardware platforms but a single hypervisor (VMM).

c) Preconditions

1) John is a subscriber of the McCloud services and has installed an OS with an IPC mechanism built on top of a McCloud proprietary inter-VM messaging service which is not based on TCP/IP.

d) Actions

1) John activates the VMI with the McCloud proprietary inter-VM messaging service supporting the hosted OS IPC service.

2) John installs and initializes an application which manages his illegal activity.

3) One of the VM contains the data which is used by the illegal activity.

4) Another VM not identifiable with John handles the login in and user interactions with other members of the illegal activity.

5) John's cohorts are then able to logon to the new VM under the standard LINUX login services that John manages.

6) The VM handling the user interface aspects communicates with the VM containing the illegal activity data VM through the IPC mechanism.

e) Results

1) Multiple VMs are involved with supporting the illegal activity. Not all of them can be linked directly with John by only examining McCloud subscriber records.

f) Challenges for interception

1) The VMI is hardware and VMM specific. The target hardware platform may be Cloud service provider specific.

2) The identities of the users of the VM may not be known to the Cloud service provider since the user identity management on the VM is by the system administrator of the hosted OS.

3) Identifying the target OS may not be known by the Cloud service provider, but require parsing the VMI.

4) To get a complete picture of the illegal activity, multiple VMs or VMIs will have to be parsed.

5) The contents of the messaging IPC between VMs is application specific. This would require reverse engineering the application running on all the VMs where the application is distributed.

A.6 Mobile Portal or Dashboard using both Operator Provided and Enterprise Applications

a) Overview

1) This use case describes a portal or dashboard which integrates access to different applications for a user for a consistent and efficient user experience. Most of these applications are not aware of the other applications integrated into the portal or dashboard interface and may not directly interact with each other. The challenge is that many of the applications can be independently deployed in many different environments.

b) Actors

1) Joe is the user. He works for Company X and is a subscriber of Operator Y. He uses the dashboard software as a productivity tool as part of his job.

2) Company X is a Fortune 500 company. Its internal Cloud based services are hosted internally.

3) Operator Y is a wireless operator. Its commercial Cloud based services are hosted internally.

c) Preconditions

1) The dashboard software operates on Joe's mobile device. It uses Cloud based email services provided by Operator Y. It uses Cloud based directory services and instant messaging provided by Company X.

2) For all applications, the application server is accessed either through an SOA framework or through a proprietary API.

3) Joe's Company X identity and credentials to access Company X services is not the same as his Operator Y identity and credentials.

4) LEA P has obtained a warrant to intercept Joe's communication through Operator Y, delivered it to Operator Y and Operator Y has activated the warrant.

5) Company X and Operator Y along with their respective Cloud service data centres are all within LEA P's legal jurisdiction.

d) Actions

1) Joe invokes the dashboard program on his smartphone while connected to Operator Y's network.

2) The dashboard program logs into both Operator Y and Company X using Joe's identity and credentials stored on the smartphone for each.

3) Joe accesses a contact group of Company X co-workers from Company X directory services that are cooperating on embezzling money from Company X.

4) Joe sends an email to the entire group indicating the invoice number and vendor that is faked using Operator Y's email service.

5) Joe initiates an IM session with one co-worker in particular using Company X's IM service.

6) Joe passes along bank and account information where to deposit the payment for the faked invoice.

7) Joe logs off of the dashboard which logs off from the various services.

8) Joe turns off his smartphone.

e) Interaction with other services

1) No interaction with other services is significant in this use case.

f) Roaming

1) Roaming does not introduce any roaming specific issues that are not already present in roaming scenarios.

g) Post Conditions

1) If the LEA has a data intercept, it will obtain any of the application specific protocol between the dashboard application and Company X and Operator Y virtual servers.

2) If the LEA has an application intercept on Operator Y email service, it will only obtain the email generated by Joe, not the directory and IM service interaction with Company X services.

h) Challenges for interception

1) It is not clear how LEA P will be able to parse or reverse engineer the client server protocols used between the dashboard and both Company X and Operator Y virtual servers in order to obtain details of the criminal activities.

2) Application intercepts are not currently defined and both the legal challenges and technical challenges such as normalizing any LI architecture and application protocol plus trying to maintain the normalized protocol in the presence of frequent application changes is significant.

A.7 Enterprise Cloud based or Dashboard using both Operator Provided and Enterprise Applications

a) Overview

1) This use case describes a portal or dashboard which integrates access to different applications for a user for a consistent and efficient user experience. Most of these applications are not aware of the other applications integrated into the portal or dashboard interface and may not directly interact with each other. The challenge is that many of the applications can be independently deployed in many different environments.

b) Actors

1) Joe is the user. He works for Company X and is a subscriber of Operator Y. He uses the dashboard software as a productivity tool as part of his job.

2) Company X is a Fortune 500 company. Its dashboard and internal Cloud based services are hosted internally.

3) Operator Y is a wireless operator. Its commercial Cloud based services are hosted internally.

c) Preconditions

1) The dashboard software is hosted on Enterprise X Cloud infrastructure and is accessed by an employee through a web browser. It uses Cloud based email services provided by Operator Y. It uses Cloud based directory services and instant messaging provided by Company X.

2) For all applications, the application server is accessed by the dashboard software either through an SOA framework or through a proprietary API.

3) Joe's Company X identity and credentials to access Company X services is not the same as his Operator Y identity and credentials.

4) LEA P has obtained a warrant to intercept Joe's communication through Operator Y, delivered it to Operator Y and Operator Y has activated the warrant.

5) Company X and Operator Y along with their respective Cloud service data centres are all within LEA P's legal jurisdiction.

d) Actions

1) Joe invokes the dashboard program on his by accessing the dashboard with his web browser and entering the appropriate URL while connected to Operator Y's network.

2) The dashboard program logs into both Operator Y and Company X using Joe's identity and credentials stored on the smartphone for each.

3) Joe accesses a contact group of Company X co-workers from Company X directory services that are cooperating on embezzling money from Company X.

4) Joe sends an email to the entire group indicating the invoice number and vendor that is faked using Operator Y's email service.

5) Joe initiates an IM session with one co-worker in particular using Company X's IM service.

6) Joe passes along bank and account information where to deposit the payment for the faked invoice.

7) Joe logs off of the dashboard which logs off from the various services.

8) Joe turns off his smartphone.

e) Interaction with other services

1) No interaction with other services is significant in this use case.

f) Roaming

1) Roaming does not introduce any roaming specific issues that are not already present in roaming scenarios.

g) Post Conditions

1) If the LEA has a data intercept, it will obtain only the http/html from the dashboard's user interface.

2) If the LEA has an application intercept on Operator Y email service, it will only obtain the email generated by Joe, not the directory and IM service interaction with Company X services.

h) Challenges for interception

1) Application intercepts are not currently defined and both the legal challenges and technical challenges such as normalizing any LI architecture and application protocol plus trying to maintain the normalized protocol in the presence of frequent application changes is significant.

A.8 Use of VDI supporting Offline Operations

a) Overview

1) This use case describes the use of VDI (Virtual Desktop Infrastructure) supporting offline operation.

b) Actors

1) Joe is the user who has subscribed to Operator O for wireless service and their VDI service.

2) Operator O is a wireless operator offering VDI services hosted in an internal Cloud environment.

c) Preconditions

1) Joe is using a PC where the local VDI components are already installed.

2) The VDI service supports local and offline operation by caching at the local machine a virtual machine environment, a virtual machine image, Joe's application in a separate cached image and Joe's user data and settings in a separate cached image.

3) The VDI service periodically (according to Operator O's policies) synchronizes the VM image, application image and user data and setting image as changes are identified.

4) LEA P has obtained a warrant to intercept Joe's communication through Operator O, delivered it to Operator O and Operator O has activated the warrant.

5) Operator O along with its Cloud service data centre is within LEA P's legal jurisdiction.

d) Actions

1) Joe logs into his PC and invokes the VDI service which logs into Operator O's VDI Cloud server.

2) The VDI Cloud service performs an initial synchronization to bring the local and centralized VMI image, application image and user data and setting image up to date.

3) Joe shuts off his wireless connection to Operator O's network.

4) Joe spends 6 hours developing plans for criminal activity.

5) Joe turns on his wireless connection to Operator O's network.

6) The VDI Cloud service again performs a synchronization to bring the local and centralized VIM image, application image and user data and setting image up to date. In this case because the local user data has changed, the VDI components send the last image to the VDI Cloud server to store.

7) Joe logs off of his PC.

e) Interaction with other services

1) No interaction with other services is significant in this use case.

f) Roaming

1) Roaming does not introduce any roaming specific issues that are not already present in roaming scenarios.

g) Post Conditions

1) Operator O will deliver to LEA P the contents of the data session synchronizing the user data and settings with Operator O's VDI Cloud server.

h) Challenges for Interception

1) It is not clear how LEA P will be able to parse or reverse engineer the user data and settings image synchronization which could be a full image or merely a delta image.

2) LEA P may also may not be able to parse or reverse engineer the user data in the synchronized image if it is in a custom format.

3) LEA P may not have all of the applicable criminal information if the user data and setting image synchronization only delivers a delta image for performance reasons.

A.9 Delayed Communication by Transferring a Cloud based Virtual Machine Image (VMI)

a) Overview

1) This use case describes a scenario where communication regarding criminal activity is composed locally, saved in a VMI. The VMI is transferred to a Cloud environment and the communication is delivered from a VM in the Cloud data centre at a later time.

b) Actors

1) Joe is the user who has subscribed to Operator O for wireless service and their IAAS service.

2) Operator O is a wireless operator offering IAAS services hosted in an internal Cloud environment as part of their Cloud service portfolio.

c) Preconditions

1) Joe is using a PC using the same hypervisor as used by Operator O's Cloud environment.

2) Joe is a subscriber of Operator O's wireless service and Cloud IAAS service.

3) LEA P has obtained a warrant to intercept Joe's communication through Operator O, delivered it to Operator O and Operator O has activated the warrant.

4) Operator O along with its Cloud service data centre is within LEA P's legal jurisdiction.

d) Actions

1) Joe starts up his PC and activates a Linux VMI in a VM.

2) Joe, on his PC records an IED making video. It is stored on a RAM disk (in memory file system).

3) Joe composes an email on his email client about when the video will be streamed and the intended location for the IED along with the email addresses of his criminal cell. The email is saved in the client's outbox on the RAM disk, but not delivered.

4) Joe creates a crontab task to start in1 hour restarting the email client to send the pending email.

5) Joe creates another crontab task to start in 4 hours to stream the IED making instructional video to the cohorts addressed in the email.

6) Joe requests the local hypervisor to take a snapshot of the VM state and save to a local disk drive.

7) Joe initiates an FTP transfer to transfer the VMI to Operator O's Cloud service, saved as a VMI in the data centre.

8) Joe starts a VM instance using the uploaded VMI.

9) Joe logs off from Operator O's network and shuts off his PC.

10) One hour later, at the VM instance, the email crontab entry is activated to start up the email client and send the composed email .

11) Three hours later, at the VM instance, the video streaming crontab entry is activated to start up the video streaming client and the IED making instructional video is streamed to the intended recipients.

12) After the video is finished, the VM instance halts.

13) The next day Joe deletes the uploaded VMI from Operator O's Cloud service centre.

e) Interactions with other services

1) No interaction with other services is significant in this use case.

f) Roaming

1) Roaming does not introduce any roaming specific issues that are not already present in roaming scenarios.

g) Post Conditions

1) Operator O will deliver to LEA P the contents of the FTP session transferring the VMI with the criminal email and video to Operator O's IAAS Cloud service.

h) Challenges for interception

1) It is not clear how LEA P will be able to parse or reverse engineer the VMI to locate the embedded criminal communication. It requires the ability to identify the RAM disk and the content structure, application specific file information as well as knowing the need to analyse the crontab tasks. Note that the active threads will not give any indication of what applications are involved in the criminal communication.

2) It is not clear how LEA P would specify LI on any communication to and from any VM running under the LI target's subscription.

3) It is not clear how LEA P would specify LI on any communication to and from any VM running a VMI created by the LI target, but activated by a different Operator O Cloud service subscriber.

A.10 Consumer based Files Sharing

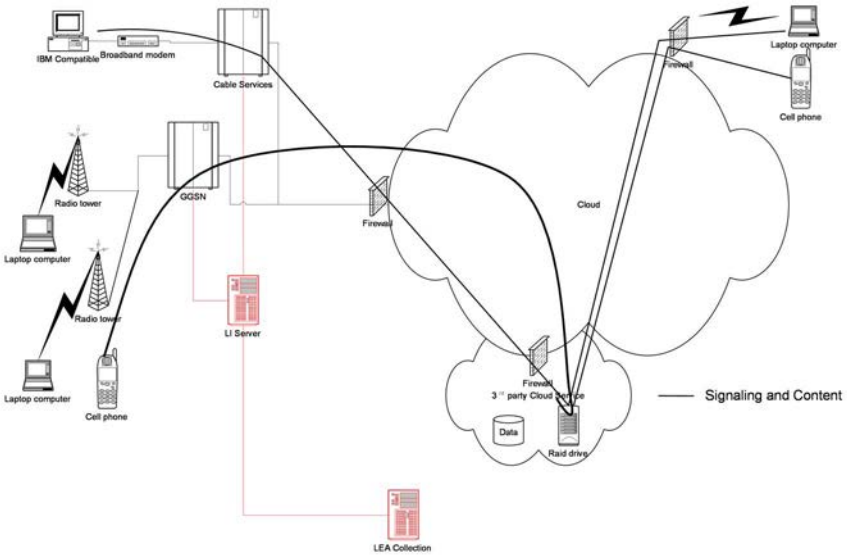


Figure A-1: Third Party Basic File Share

a) Overview

1) The user installed a File Sharing application on their mobile device.

2) The MNO only allows access to File Sharing services.

a. The service and facilities supporting the service are located external to the MNO domain.

b) Actors

1) John is a user.

2) Regional Mobile is a MNO that only allows mobile service in the Domain of 3pp-istan.

3) AlsoRan is a vendor of 3GPP infrastructure.

4) Mega Cloud is a Global Cloud infrastructure provider.

5) Third Party Application provider "File Drop" is not related to any of the actors, it may have a relationship with Mega Cloud or an agent of Mega Cloud to host its Application.

c) Preconditions

1) John lives in 3pp-istan and is a subscriber of Regional Mobile.

2) John has selected the File Sharing service from a third party File Drop. The service allows John to share files only between users and devices that have a subscription on third party. The service provides encrypted services and access to other networks users including the Public. The service is limited to 2 Gigabytes of storage. The use of the feature to move or retrieve files to or from the Cloud does consume access service plan with Regional Mobile. John can subscribe to larger storage plans.

3) The Third party application does not manage access to shared files. Its client software provides a link address where the file is stored. Anyone with the link can access the file. Access to the File share system is via simple user name and password and can be stored in the client.

4) The File Sharing Application is from a third party that is using resources on Mega Cloud. Those resources may have been contracted directly or through other agents and or application providers.

d) Actions

1) John selects the application from his device. And enters user name and password, if not previously saved.

2) The application displays a directory system of his file share system, showing Private and public directories and the files in each.

3) John transfers from his device memory a file to the client application.

4) John selects to move the file to the Private folder, the client application, uploads to File Drop a copy of the file

5) John selects another file, one with which he intends to commit an unlawful act and moves it to the Public folder.

6) The client uploads to File Drop a copy of the file and a file locator is returned.

7) John copies the file locator information and sends an SMS to an associate including the file locator information.

8) The associate upon receipt of the SMS, copies the file locator to his client application and retrieves the file.

9) John selects a different device that has the file share application enabled.

10) John logs into the File share systems with this device and the application determines that this devices needs to sync with the system and down loads one file to the local private director (mirror on the device) and one to the Public folder.

11) Sometime later John deletes the file from his shared folder (public).

12) Sometime later John will notice that all devices that are logged in to the File Share application will have this file removed from its local device memory.

13) A device that is not connected to the internet and not able to connect to the application will still retain a copy of the file until it is synchronized with the server.

Variation A

1 to 7 the same.

8) The associated upon receipt of the SMS, forwards it to another associated who then copies the file locator to his client application and retrieves the file.

9) Sometime later John deletes the file from his shared folder.

Variation B

1 to 5 the same.

6) The client request John to enter in SMS and or email address of individuals to share the content. This information is received by File Drop Server which then sends a unique message to each recipient.

7) The associate upon receipt of the SMS or email, copies the message to his client application.

8) The File Drop server checks the unique message against (non exhaustive list, sms MSIDN, email address, log in credentials of the file share and) other server information to determine validly of the user accessing the file.

9) Upon successful validation delivers a copy of the file.

Variations to B

1) File Drop server provides an indication when someone has accessed the shared files.

2) John deletes the files from his shared folder.

e) Interaction with other services

1) The file Share may be part of an interactive service like social media, email, where updates are sent.

2) It may be possible to access the files from social media sites.

3) It may be possible to delete files via Email commands sent to the server.

4) Local break with Femto cell and access to local shares and or use of Cellular Hub (cellular modem that terminates in wifi or Ethernet access) on John's personal network is for further study.

f) Roaming

1) When John roams to other networks, his File share travels with him and is accessible. Roaming Rates for data services may apply.

2) Local Break out services in the visited network does not support access to the file share that is in Regional Mobile.

g) Results

1) John and his associates have shared a file that has or will be used in an unlawful act.

2) John and the associates may have tried to hide any transactions.

3) Regional Mobile can only provide the basic IRI of the data session and the encrypted file content to LEA.

h) Challenges for interception

1) Generally in this use case if a Warrant is effect at the time that John uploads the file, LEA will get basic IRI on the data session and encrypt content of the session with File Drop service. It will capture the SMS sent by John.

2) It is not clear if LEA will receive information on others accessing the File share during the warrant period.

A.11 Consumer based File Sharing 1

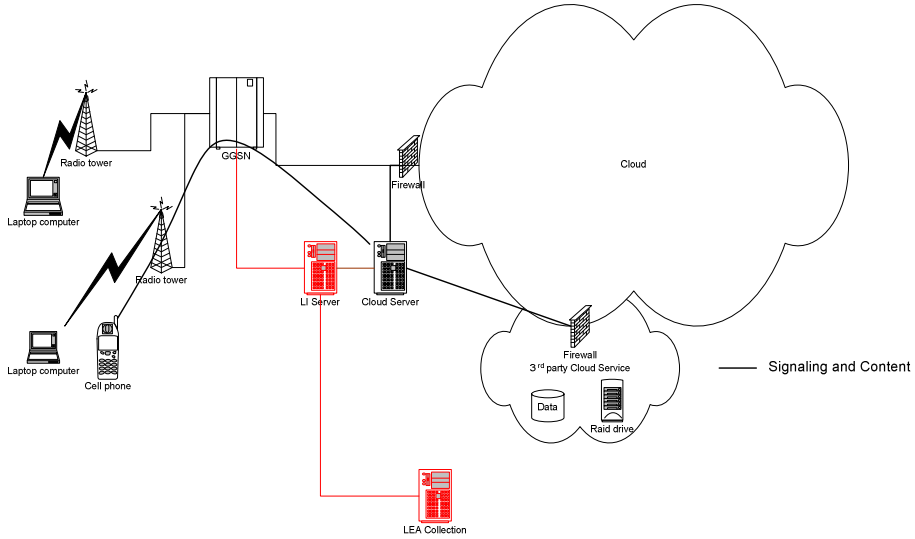


Figure A-2: MNO Proxies Cloud Services; File Share

a) Overview

1) The MNO only allows access to File Sharing services only to subscribers of the service while on the MNO facilities and not accessible from Non 3GPP access networks.

a. The service and facilities supporting the service are located within the MNO domain.

b. The Facilities are external to the MNO domain but only accessible via the MNO domain.

c. The service can be offered with or without IMS services.

2) Similar services: MNO Network Address Book (White pages), SMB Address Book.

b) Actors

1) John is a user.

2) Scott is a user and an associate of John.

3) Joan is a user and an associate of John.

4) Regional Mobile is a MNO that only allows mobile service in the Domain of 3pp-istan.

5) AlsoRan is a vendor of 3GPP infrastructure.

c) Preconditions

1) John lives in 3pp-istan and is a subscriber of Regional Mobile and has selected the File Sharing service. The service allows John to share files only between users and devices that have a subscription on Regional Mobile. The service does not provide encrypted services and no access to other networks users including the Public. The service is limited to 2 Gigabytes of storage. The use of the feature to move or retrieve files to or from the Cloud does not consume any access service plan. John can subscribe to larger storage plans.

2) Regional Mobile has contracted with its vendor AlsoRan to provide the service. AlsoRan provides a client that can operate on Mobile devices (smart phones, tablets and laptops).

3) AlsoRan does not manage access to shared files. Its client software provides a link address where the file is stored. Anyone with the link can access the file. Access to the File share system is via simple user name and password and can be stored in the client.

d) Actions

1) The Regional Mobile surveillance facilities identify that a target of LI has initiated communication covered by the LI authorization and begins delivery of the communication to the LEA.

2) The 3gpp-istan Police Department begins receiving John's intercepted communications (i.e. IRI and CC for all required services as identified in the lawful authorization). The IRI and CC for the Consumer File Sharing service is delivered separately and the CC is the media that is sent to/from John (the Subject).

3) John selects the application from his device. And enters user name and password, if not previously saved.

4) The application displays a directory system of his file share system, showing Private and public directories and the files in each.

5) John transfers from his device memory a file to the client application.

6) John selects to move the file to the Private folder, the client application, uploads to AlsoRan a copy of the file.

7) John selects another file, one with which he intends to commit an unlawful act and moves it to the Public folder.

8) The client uploads to AlsoRan a copy of the file and a file locator is returned.

9) John copies the file locator information and sends an SMS to an associate including the file locator information.

10) The associate. Scott (who also is a subscriber of Regional Mobile) upon receipt of the SMS, copies the file locator to his client application and retrieves the file.

11) John selects a different device that has the file share application enabled.

12) John logs into the File share systems with this device and the application determines that this devices needs to sync with the system and down loads one file to the local private director (mirror on the device) and one to the Public folder.

13) Sometime later John deletes the file from his shared folder (public).

14) Sometime later John will notice that all devices that are logged in to the File Share application will have this file removed from its local device memory.

15) A device that is not connected to the MNO network and not able to connect to the application will still retain a copy of the file until it is synchronized with the server.

Variations A

1 to 9 the same.

10) The associate Scott (who also is a subscriber of Regional Mobile) upon receipt of the SMS, forwards it to another associate Joan who then copies the file locator to her client application and retrieves the file.

11) Sometime later John deletes the file from his shared folder.

Variations B

1 to 8 the same.

9) The client request John to enter in SMS and or email address of individuals to share the content. This information is received by AlsoRan Server which then sends a unique message to each recipient.

10) The associate Scott (who also is a subscriber of Regional Mobile) upon receipt of the SMS or email, copies the message to his client application.

11) The AlsoRan server checks the unique message against (non exhaustive list, sms MSIDN, email address, log in credentials of the file share and) other server information to determine validly of the user accessing the file.

12) Upon successful validation delivers a copy of the file.

Variations to B

1) AlsoRan server provides an indication when someone has accessed the shared files.

2) John deletes the files from his shared folder.

e) Interaction with other services

1) The file Share may be part of an interactive Messaging platform, where all files are stored, voice mail, video mail and shared files.

2) It may be possible to access the shared folder via tele-prompts in the Messaging centre.

3) It may be possible to access the system via Web Browser client through the MNO's Web Portal.

4) It may be possible to delete files via Email commands sent to the server.

5) Local break with Femto cell and access to local shares and or use of Cellular Hub (cellular modem that terminates in wifi or Ethernet access) on John's personal network is for further study.

f) Roaming

1) When John roams to other networks, his File share travels with him and is accessible. Roaming Rates for data services may apply.

2) John could send a SMS or email to others with a file location to people not subscribers to Regional Mobile, however they would receive an error message.

3) Local Break out services in the visited network does not support access to the file share that is in Regional Mobile.

g) Post Conditions

1) John and his associates Scott and Joan have shared a file that has or will be used in an unlawful act.

2) John and the associates Scott and Joan may have tried to hide any transactions.

3) The 3gpp-istan Police Department received the IRI and CC of John's communications. Using that information in their investigations, they prevent a crime from occurring.

4) Regional Mobile met their regulatory obligation to unobtrusively deliver communication to the authorized LEA.

h) Challenges for interception

1) Generally in this use case if a Warrant is effect at the time that John uploads the file, LEA should receive all related information.

2) It is not clear if LEA will receive information on others accessing the File share during the warrant period.

3) If a warrant is not in effect when John uploads the file, it is not clear whether LI systems are capable of capturing the retrieval by associates when a warrant is issued.

4) For specific implementations it is not clear if the system can identify the user accessing the shared file.

5) It is not clear if other means to delete the file can be captured.

6) It is not clear how long AlsoRan will need to preserve the contents of the file and its associated logs (business records, Data Storage).

7) Issue of file de-publication (i.e. pointers to one storage of a file).

8) How and what data/ IRI is presented to LEA (e.g. service type, clear text files).

A.12 Consumer based File Sharing 2

The Cloud function are in a different LEA jurisdictions.

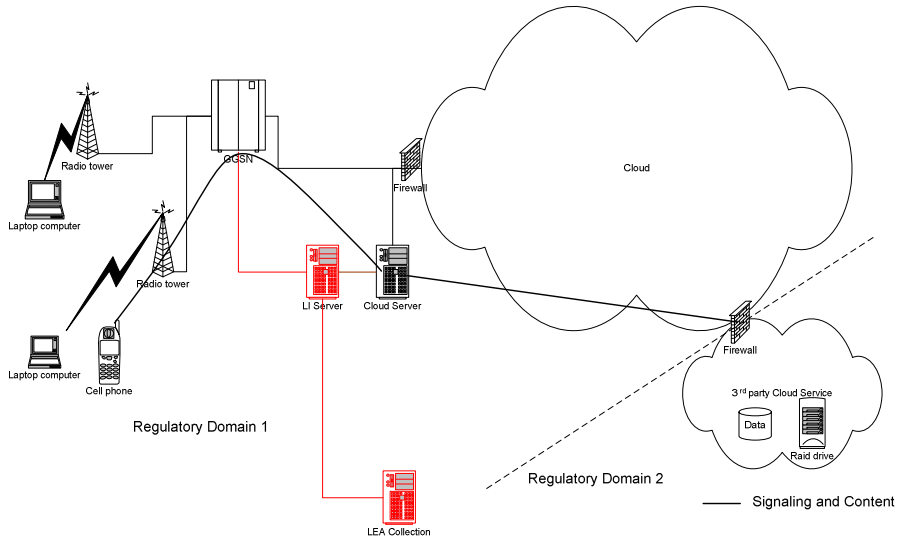


Figure A-3: MNO Proxies Cloud; File Share, located in different regulatory Domain

a) Overview

1) The MNO only allows access to File Sharing services only to subscribers of the service while on the MNO facilities and not accessible from Non 3GPP access networks:

a. The service and facilities supporting the service are located within the MNO domain.

b. The Facilities are external to the MNO domain but only accessible via the MNO domain.

c. The service can be offered with or without IMS services.

b) Actors

1) The user is John.

2) Scott is a user and an associate of John.

3) Joan is a user and an associate of John.

4) Regional Mobile is a MNO that only allows mobile service in the Domain of 3pp-istan.

5) McCloud is a Cloud Service Provider in the Domain of Inter-istan.

6) Thunder-Cloud is a vendor or Cloud computing infrastructure in the Domain of Inter-istan.

c) Preconditions

1) John lives in 3pp-istan and is a subscriber Regional Mobile and has selected the File Sharing service. The service allows John to share files only between users and devices that have a subscription on Regional Mobile. The service does not provide encrypted services and no access other networks including the Public. The service is limited to 2 Gigabytes of storage. The use of the feature to move or retrieve files to or from the Cloud does not consume any access service plan. John can subscribe to larger storage plans.

2) Regional Mobile has contracted with McCloud to provide the service. McCloud provides a client that can operate on Mobile devices (smart phones, tablets and laptops).

3) McCloud does not manage access to shared files. Its client software provides a link address where the file is stored. Anyone with the link can access the file. Access to the File share system is via simple user name and password and can be stored in the client.

4) McCloud contracts with Thunder-Cloud to provide infrastructure to hosts it service.

5) Regional Mobile redirects all requests to these File Share services to McCloud using its internal DNS server within Regional Mobile.

6) McCloud maintains a data base to map IP address to determine the MNO and Users.

7) McCloud and or Thunder-Cloud may protect the User data.

d) Actions

1) The Regional Mobile surveillance facilities identify that a target of LI has initiated communication covered by the LI authorization and begins delivery of the communication to the LEA.

2) The 3gpp-istan Police Department begins receiving John's intercepted communications (i.e. IRI and CC for all required services as identified in the lawful authorization). The IRI and CC for the Consumer File Sharing service is delivered separately and the CC is the media that is sent to/from John (the Subject).

3) John selects the application from his device. And enters user name and password, if not previously saved, it connects to the McCloud Server.

4) The McCloud Application server provides temporary IP addresses for the Thunder Cloud infrastructure that is hosting the file service at that instance.

5) The application connects to the Thundercloud infrastructure and McCloud application running there.

6) The application displays a directory system of his file share system, showing Private and public directories and the files in each.

7) John transfers from his device memory a file to the client application.

8) John selects to move the file to the Private folder, the client application, uploads to McCloud application a copy of the file.

9) John selects another file, one with which he intends to commit an unlawful act and moves it to the Public folder.

10) The client uploads a copy of the file and a file locator is returned.

11) John copies the file locator information and sends an SMS to an associate including the file locator information.

12) The associate Scott (who also is a subscriber of Regional Mobile) upon receipt of the SMS, copies the file locator to his client application and retrieves the file.

13) John selects a different device that has the file share application enabled.

14) John logs into the File share systems with this device and the application determines that this devices needs to sync with the system and down loads one file to the local private director (mirror on the device) and one to the Public folder.

15) Sometime later John deletes the file from his shared folder (public).

16) Sometime later John will notice that all devices that are logged in to the File Share application will have this file removed from its local device memory.

17) A device that is not connected to the MNO network and not able to connect to the application will still retain a copy of the file until it is synchronized with the server.

Variations A

1 to 11 the same.

12) The associated Scott (who also is a subscriber of Regional Mobile) upon receipt of the SMS, forwards it to another associate Joan who then copies the file locator to her client application and retrieves the file.

13) Sometime later John deletes the file from his shared folder.

Variations B

1 to 10 the same.

11) The client request John to enter in SMS and or email address of individuals to share the content. This information is received by McCloud Server which then sends a unique messages to each recipient.

12) The associate Scott (who also is a subscriber of Regional Mobile) upon receipt of the SMS or email, copies the message to his client application.

13) The McCloud application checks the unique message against (non-exhaustive list, sms MSIDN, email address, log in credentials of the file share and) other server information to determine validly of the user accessing the file.

14) Upon successful validation delivers a copy of the file.

Variations to B

1) McCloud server provides an indication when someone has accessed the shared files.

2) John deletes the files from his shared folder.

e) Interaction with other services

1) The file Share may be part of an interactive Messaging platform, where all files are stored, voice mail, video mail and shared files.

2) It may be possible to access the shared folder via tele-prompts in the Messaging centre.

3) It may be possible to access the system via Web Browser client through the MNO's Web Portal.

4) It may be possible to delete files via Email commands sent to the server.

5) Local break with Femto cell and access to local shares and or use of Cellular Hub (cellular modem that terminates in Wi-Fi or Ethernet access) on John's personal network is for further study.

f) Roaming

1) When John roams to other networks, his File share travels with him and is accessible. Roaming Rates for data services may apply.

2) John could send a SMS or email to others with a file location to people not subscribers to Regional Mobile, however they would receive an error messages.

3) Local Break out services in the visited network does not support access to the file share that is in Regional Mobile.

g) Post Conditions

1) John and his associates Scott and Joan have shared a file that has or will be used in an unlawful act.

2) John and the associates Scott and Joan may have tried to hide any transactions.

3) The 3gpp-istan Police Department received the IRI and CC of John's communications. Using that information in their investigations, they prevent a crime from occurring.

4) Regional Mobile met their regulatory obligation to unobtrusively deliver communication to the authorized LEA.

h) Challenges for interception

1) Generally in this use case if a Warrant is effect at the time that John uploads the file, LEA should receive all related information.

2) It is not clear if LEA will receive information on others accessing the File share during the warrant period.

3) If a warrant is not in effect when John uploads the file, it is not clear whether LI systems are capable of capturing the retrieval by associates when a warrant is issued.

4) It is not clear if the system can identify the user accessing the shared file.

5) It is not clear if other means to delete the file can be captured.

6) It is not clear how LEA will access the files in McCloud and or Thunder Cloud systems will need to preserve the contents of the file and its associated logs (business records, Data Storage).

7) The files are accessible to LEA in Inter-istan, although it is unclear on the relationship to John and the file server User ID used, Regional Mobile may only have this information.

8) Issue of file de-publication (i.e. pointers to one storage of a file).

9) How and what data/ IRI is presented to LEA (e.g. service type, clear text files).

A.13 Consumer based File Sharing 3

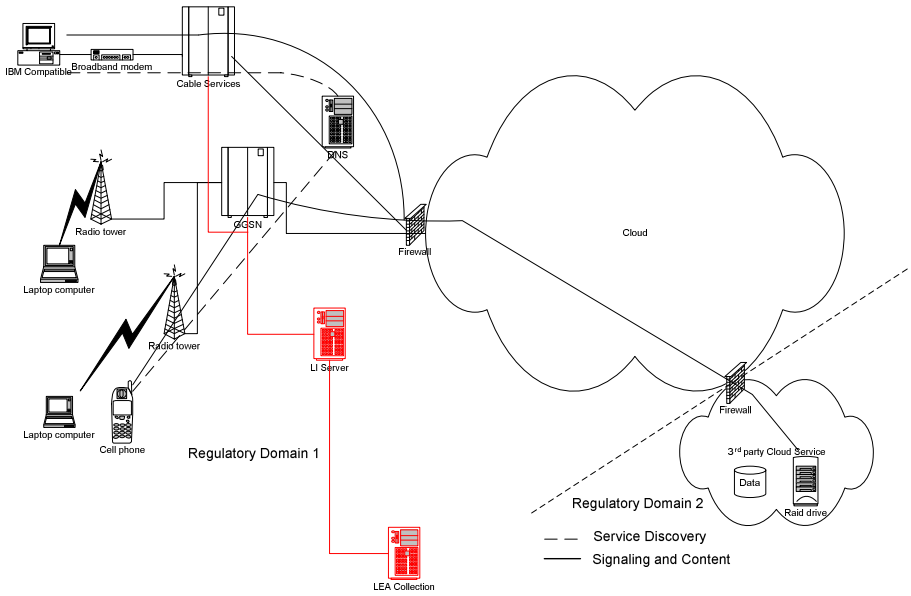


Figure A-4: MNO local Cloud discovery; File Share, located in different Regulatory Domain

a) Overview

1) The MNO only allows access to File Sharing services only to subscribers of the service while on the MNO facilities and not accessible from Non 3GPP access networks.

a. The Facilities are external to the MNO domain but only accessible via the MNO domain.

b. The service can be offered with or without IMS services.

b) Actors

1) The user is John.

2) Scott is a user and an associate of John.

3) Joan is a user and an associate of John.

4) Regional Mobile is a MNO that only allows mobile service in the Domain of 3pp-istan.

5) McCloud is a Cloud Service Provider in the Domain of Inter-istan.

6) Thunder-Cloud is a vendor or Cloud computing infrastructure in the Domain of Inter-istan.

c) Preconditions

1) John lives in 3pp-istan and is a subscriber Regional Mobile and has selected the File Sharing service. The service allows John to share files only between users and devices that have a subscription on Regional Mobile. The service does not provide encrypted services and no access other networks including the Public. The service is limited to 2 Gigabytes of storage. The use of the feature to move or retrieve files to or from the Cloud does not consume any access service plan. John can subscribe to larger storage plans.

2) Regional Mobile has contracted with McCloud to provide the service. McCloud provides a client that can operate on Mobile devices (smart phones, tablets and laptops).

3) McCloud does not manage access to shared files. Its client software provides a link address where the file is stored. Anyone with the link can access the file. Access to the File share system is via simple user name and password and can be stored in the client.

4) McCloud contracts with Thunder-Cloud to provide infrastructure to hosts it service.

5) Regional Mobile redirects all requests to these File Share services to McCloud using its internal DNS server within Regional Mobile.

6) McCloud maintains a data base to map IP address to determine the MNO and Users.

7) McCloud and or Thunder-Cloud may protect the User data.

d) Actions

1) The Regional Mobile surveillance facilities identify that a target of LI has initiated communication covered by the LI authorization and begins delivery of the communication to the LEA.

2) The 3gpp-istan Police Department begins receiving John's intercepted communications (i.e. IRI and CC for all required services as identified in the lawful authorization). The IRI and CC for the Consumer File Sharing service is delivered separately and the CC is the media that is sent to/from John (the Subject).

3) John selects the application from his device. And enters user name and password, if not previously saved, it connects to the McCloud Server.

4) The McCloud Application server provides temporary IP addresses for the Thunder Cloud infrastructure that is hosting the file service at that instance.

5) The application connects to the Thundercloud infrastructure and McCloud application running there.

6) The application displays a directory system of his file share system, showing Private and public directories and the files in each.

7) John transfers from his device memory a file to the client application.

8) John selects to move the file to the Private folder, the client application, uploads to McCloud application a copy of the file.

9) John selects another file, one with which he intends to commit an unlawful act and moves it to the Public folder.

10) The client uploads a copy of the file and a file locator is returned which contains a FQDN address.

11) John copies the file locator information and sends an SMS to an associate including the file locator information.

12) The associate Scott (who also is a subscriber of Regional Mobile) upon receipt of the SMS, copies the file locator to his client application and retrieves the file.

13) John selects a different device that has the file share application enabled.

14) John logs into the File share systems with this device and the application determines that this devices needs to sync with the system and down loads one file to the local private director (mirror on the device) and one to the Public folder.

15) Sometime later John deletes the file from his shared folder (public).

16) Sometime later John will notice that all devices that are logged in to the File Share application will have this file removed from its local device memory.

17) A device that is not connected to the MNO network and not able to connect to the application will still retain a copy of the file until it is synchronized with the server.

Variation A

1 to 11 the same.

12) The associate Scott (who also is a subscriber of Regional Mobile) upon receipt of the SMS, forwards it to another associate Joan who then copies the file locator to his client application and retrieves the file.

13) Sometime later John deletes the file from his shared folder.

Variation B

1 to 11 the same.

12) The associate Scott (who also is a subscriber of Regional Mobile) upon receipt of the SMS, forwards it to another associate Joan (who is not a subscriber of Regional Mobile) who then copies the file locator to his client application and attempts to retrieves the file.

13) If Mc Cloud and Thunder Cloud check source IP addresses, they will determine it is not coming from Regional Mobile and deny access.

14) Sometime later John deletes the file from his shared folder.

Variation C

1 to 10 the same.

11) The client request John to enter in SMS and or email address of individuals to share the content. This information is received by McCloud Server which then sends a unique message to each recipient.

12) The associate Scott (who also is a subscriber of Regional Mobile) upon receipt of the SMS or email, copies the message to his client application.

13) The McCloud application checks the unique message against (non-exhaustive list, sms MSIDN, email address, log in credentials of the file share and) other server information to determine validly of the user accessing the file.

14) Upon successful validation delivers a copy of the file.

Variations to C

1 to 10 the same.

11) The associate Scott (who also is a subscriber of Regional Mobile) upon receipt of the SMS, forwards it to another associate Joan (who is not a subscriber of Regional Mobile) who then copies the file locator to his client application and attempts to retrieves the file.

12) Mc Cloud and Thunder Cloud should deny access based upon unique message and or source IP.

13) Sometime later John deletes the file from his shared folder.

Variations to B

1) McCloud server provides an indication when some has accessed the shared files.

2) John deletes the files from his shared folder.

e) Interaction with other services

1) The file Share may be part of an interactive Messaging platform, where all files are stored, voice mail, video mail and shared files.

2) It may be possible to access the shared folder via tele-prompts in the Messaging centre.

3) It may be possible to access the system via Web Browser client through the MNO's Web Portal.

4) It may be possible to delete files via Email commands sent to the server.

5) Local break with Femto cell and access to local shares and or use of Cellular Hub (cellular modem that terminates in wifi or Ethernet access) on John's personal network is for further study.

f) Roaming

1) When John roams to other networks, his File share travels with him and is accessible. Roaming Rates for data services may apply.

2) John could send a SMS or email to others with a file location to people not subscribers to Regional Mobile; however they would receive an error messages.

3) Local Break out services in the visited network does not support access to the file share that is in Regional Mobile.

g) Post Conditions

1) John and his associates Scott and Joan have shared a file that has or will be used in an unlawful act.

2) John and the associates Scott and Joan may have tried to hide any transactions.

3) The 3gpp-istan Police Department received the IRI and CC of John's communications. Using that information in their investigations, they prevent a crime from occurring.

4) Regional Mobile met their regulatory obligation to unobtrusively deliver communication to the authorized LEA.

h) Challenges for interception

1) Generally in this use case if a Warrant is effect at the time that John uploads the file, LEA should receive all related information.

2) It is not clear if LEA will receive information on others accessing the File share during the warrant period.

3) If a warrant is not in effect when John uploads the file, it is not clear whether LI systems are capable of capturing the retrieval by associates when a warrant is issued.

4) It is not clear if the system can identify the user accessing the shared file.

5) It is not clear how attempts to access the file are communicated to LEA (FQDN access via other networks).

6) For specific implementations it is not clear if other means to delete the file can be captured.

7) It is not clear how LEA will access the files in McCloud and or Thunder Cloud systems will need to preserve the contents of the file and its associated logs (business records, Data Storage).

8) The files are accessible to LEA in Inter-istan, although it is unclear on the relationship to John and the file server User ID used, Regional Mobile may only have this information.

9) Issue of file de-publication (i.e. pointers to one storage of a file).

10) How and what data/ IRI is presented to LEA (e.g. service type, clear text files).

A.14 Consumer based File Sharing 4

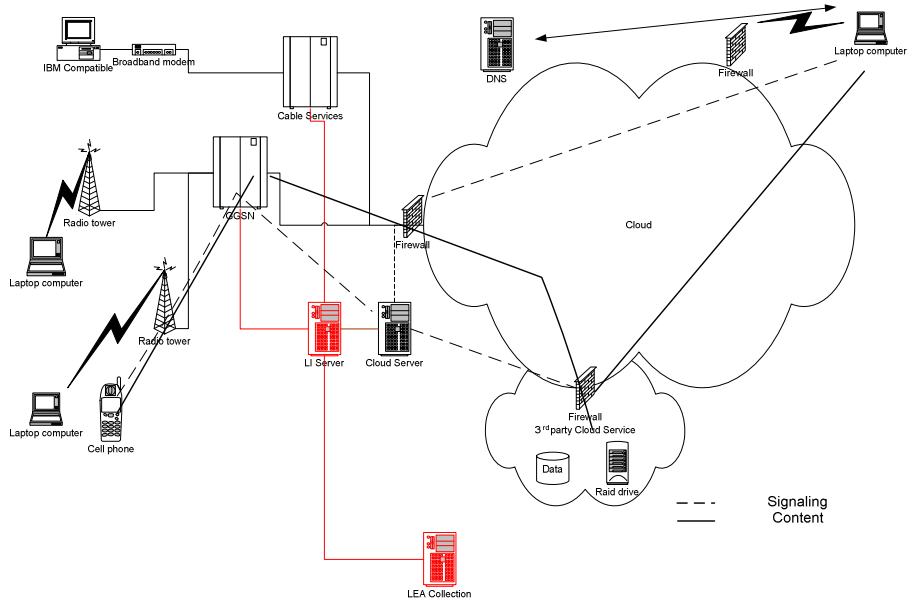


Figure A-5: MNO Cloud Proxy

a) Overview

1) The MNO only allows access to File Sharing services only to subscribers of the service while on the MNO facilities or from Non 3GPP Access Domains.

b) Actors

1) The user is Mary.

2) Brad is a user and an associate of Mary.

3) Joan is a user and an associate of Mary.

4) Mobile Anywhere is an MNO that provides access services on Mobile, fixed and broadband networks in the Domain of 3ppistan.

5) AlsoRan is a vendor of 3GPP infrastructure.

c) Preconditions

1) Mary lives in 3pp-istan and is a subscriber Mobile Anywhere and has selected the File Sharing service. The service allows Mary to share files between users and devices that have a client or web access. The service does provide encrypted services and access other networks including the Public. The service is limited to 2 Gigabytes of storage. The use of the feature to move or retrieve files to or from the Cloud does not consume any access service plan. Mary can subscribe to larger storage plans.

2) Mobile Anywhere has contracted with its vendor AlsoRan to provide the service. AlsoRan provides a client that can operate on Mobile devices (smart phones, tablets and laptops).

3) AlsoRan does not manage access to shared files. Its client software provides a link address (URL) where the file is stored. Anyone with the link can access the file. Access to the File share system is via simple user name and password and is accessible via the public Internet.

d) Actions

1) The Mobile Anywhere surveillance facilities identify that a target of LI has initiated communication covered by the LI authorization and begins delivery of the communication to the LEA.

2) The 3gpp-istan Police Department begins receiving John's intercepted communications (i.e. IRI and CC for all required services as identified in the lawful authorization). The IRI and CC for the Consumer File Sharing service is delivered separately and the CC is the media that is sent to/from John (the Subject).

3) Mary selects the application from her device. And enters user name and password, if not previously saved.

4) The application displays a directory system of her file share system, showing Private and public directories and the files in each.

5) Mary transfers from her device memory a file to the client application.

6) Mary selects to move the file to the Private folder, the client application, uploads to AlsoRan a copy of the file.

7) Mary selects another file, one with which she intends to commit an unlawful act and moves it to the Public folder.

8) The client uploads to AlsoRan a copy of the file and a file locator is returned.

9) Mary copies the file locator information and sends an SMS to an associate including the file locator information.

10) The associate Brad (who also is a subscriber of Mobile Anywhere) upon receipt of the SMS, copies the file locator to her client application and retrieves the file.

11) Mary selects a different device that has the file share application enabled.

12) Mary logs into the File share systems with the device and the application determines that this devices needs to sync with the system and down loads one file to the local private director (mirror on the device) and one to the Public folder.

13) Sometime later Mary deletes the file from her shared folder (public).

14) Sometime later Mary will notice that all devices that are logged in to the File Share application will have this file removed from its local device memory.

15) A device that is not connected to the MNO network and not able to connect to the application will still retain a copy of the file until it is synchronized with the server.

Variation A

1 to 9 the same.

10) The associate Brad (who also is a subscriber of Mobile Anywhere) upon receipt of the SMS, forwards it to another associate Joan (who is not a subscriber to Mobile Anywhere) who then copies the file locator to their client application and retrieves the file.

11) Sometime later Mary deletes the file from her shared folder.

Variation B

1 to 8 the same.

9) The client request Mary to enter in SMS and or email address of individuals to share the content. This information is received by AlsoRan Server which then sends a unique message to each recipient.

10) The associate Brad (who also is a subscriber of Mobile Anywhere) upon receipt of the SMS or email, copies the message to her client application.

11) The associate Joan (who subscriber of Regional Mobile) upon receipt of the SMS or email, copies the message to her client application.

12) The AlsoRan server checks the unique message against (non-exhaustive list, sms MSIDN, email address, log in credentials of the file share and) other server information to determine validly of the user accessing the file.

13) Upon successful validation delivers a copy of the file.

Variations to B

1) AlsoRan server provides an indication when someone has accessed the shared files.

2) Mary deletes the files from her shared folder.

e) Interaction with other services

1) The file Share may be part of an interactive Messaging platform, where all files are stored, voice mail, video mail and shared files.

2) It may be possible to access the shared folder via tele-prompts in the Messaging centre.

3) It may be possible to access the system via Web Browser client through the MNO's Web Portal.

4) It may be possible to delete files via Email commands sent to the server.

5) Local break with Femto cell and access to local shares and or use of Cellular Hub (cellular modem that terminates in wifi or Ethernet access) on Mary's personal network is for further study.

f) Roaming

1) When Mary roams to other networks, her File share travels with her and is accessible. Roaming Rates for data services may apply.

2) Mary could send a SMS or email to others with a file location to people not subscribers to Mobile Anywhere,

3) Local Break out services in the visited network does not support access to the file share that is in Regional Mobile.

g) Post Conditions

1) Mary and her associates Brad and Joan have shared a file that has or will be used in an unlawful act.

2) Mary and the associates may have tried to hide any transactions.

3) The 3gpp-istan Police Department received the IRI and CC of John's communications. Using that information in their investigations, they prevent a crime from occurring.

4) Mobile Anywhere met their regulatory obligation to unobtrusively deliver communication to the authorized LEA.

h) Challenges for interception

1) Generally in this use case if a Warrant is effect at the time that Mary uploads the file, LEA may receive all related information.

2) Location of the IAP.

3) It is not clear if LEA will receive information on others accessing the File share during the warrant period.

4) If a warrant is not in effect when Mary uploads the file, it is not clear whether LI systems are capable of capturing the retrieval by associates when a warrant is issued.

5) It is not clear if the system can identify the user accessing the shared file

   a. Cellular user from different MNO

   b. IP user

6) For specific implementations it is not clear if other means to delete the file can be captured.

7) It is not clear how long AlsoRan will need to preserve the contents of the file and its associated logs (business records, Data Storage).

8) The encryption issues are as per other use cases.

9) Issue of file de-publication (i.e. pointers to one storage of a file).

10) How and what data/ IRI is presented to LEA (e.g. service type, clear text files).

A.15 Consumer based File Sharing 5

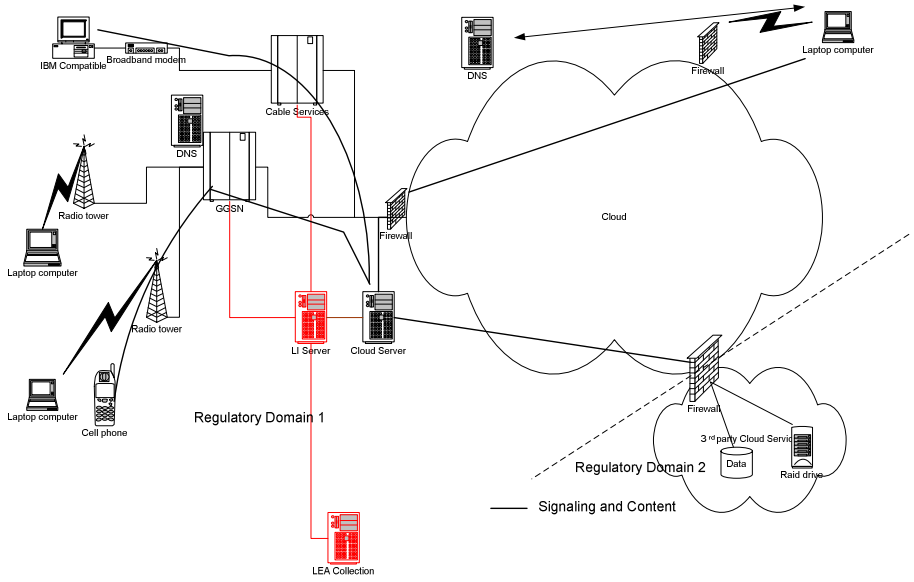


Figure A-6: MNO Cloud Proxy with service in different Regulatory Domain

a) Overview

1) The MNO only allows access to File Sharing services only to subscribers of the service while on the MNO facilities or from Non 3GPP access networks.

a. The Facilities are external to the MNO domain but only accessible via the MNO domain.

b. The service can be offered with or without IMS services.

b) Actors

1) The user is Mary.

2) Brad is a user and an associate of Mary.

3) Joan is a user and an associate of Mary.

4) Joan has a subscription to the Cloud Service offered by Mobile Anywhere.

5) Gabor is an associate of Mary, Gabor does not have any affiliations with Mobile Anywhere.

6) Mobile Anywhere, is an MNO that provides access services on Mobile, fixed and broadband networks in the Domain of 3ppistan.

7) AlsoRan is a vendor of 3GPP infrastructure.

8) Regional Mobile is a MNO that only allows mobile service in the Domain of 3pp-istan.

9) McCloud is a Cloud Service Provider in the Domain of Inter-istan.

10) Thunder-Cloud is a vendor or Cloud computing infrastructure in the Domain of Inter-istan.

c) Preconditions

1) Mary lives in 3pp-istan and is a subscriber Mobile Anywhere and has selected the File Sharing service. The service allows Mary to share files only between users and devices that have a subscription on Mobile Anywhere. A subscription is available to web access only subscribers not having any other services with Mobile Anywhere except the File Sharing service. The service does not provide encrypted services. The service is limited to 2 Gigabytes of storage. The use of the feature to move or retrieve files to or from the Cloud does not consume any access service plan. Mary can subscribe to larger storage plans.

2) Mobile Anywhere has contracted with McCloud to provide the service (File Sharing). Mobile Anywhere uses a Cloud Services Application from its Infrastructure Vendor AlsoRan. The Cloud Service Application can support many Cloud Services and provides Mobile Anywhere with integration interface to these services and the vendors that may be used to provide service.

3) AlsoRan provides a client that can operate on devices (smart phones, tablets and laptops) and the NNI, (Network to Network Interface) with McCloud. AlsoRan may hide the user's identity from McCloud.

4) McCloud does not manage access to shared files. Its client software provides a link address where the file is stored. Anyone with the link can access the file. Access to the File share system is via simple user name and password and can be stored in the client.

5) McCloud contracts with Thunder-Cloud to provide infrastructure to hosts it service. Thunder-Cloud and McCloud reside in Inter-istan.

6) Mobile Anywhere utilizes an FQDN to address the Cloud Service and redirects all requests to these File Share services to AlsoRAN Cloud Service Application Server using its internal DNS server within Mobile Anywhere. External requests are directed to the appropriate Firewalls in Mobile Anywhere and to the Cloud Service Application Server.

7) The Cloud Service Application requires User logon in order to access the File Share application.

8) The Cloud Service Application may locally manage the subscriber information an store all users files as unique files as Mobile Anywhere files, hiding all users from McCloud.

9) Through the NII, several parameters may be utilized in Mobile Anywhere's deployment.

   a. Time to Live parameters, upon access of file

   b. Logon

   c. OAM Functionality

   d. Remote management of the service

   e. Access to files

   f. Access to unencrypted files

   g. Crypto keys to use

   h. Link Security.

   i. Quality of Service / Experience

10) McCloud maintains an NNI to Mobile Anywhere, it may maintain a data base of MNO and or of MNO and its Users. It may provide back up and restoration features.

11) McCloud and or Thunder-Cloud may protect the MNO and or User data.

12) AlsoRan may encrypt the files it stores with McCloud. These may be one key for all files or individual keys for each subscriber. Mobile Anywhere through AlsoRan manages these keys and are not provided to the subscriber.

d) Actions

1) The Mobile Anywhere surveillance facilities identify that a target of LI has initiated communication covered by the LI authorization and begins delivery of the communication to the LEA.

2) The 3gpp-istan Police Department begins receiving Mary's intercepted communications (i.e. IRI and CC for all required services as identified in the lawful authorization). The IRI and CC for the Consumer File Sharing service is delivered separately and the CC is the media that is sent to/from Mary (the Subject).

3) Mary selects the application from her device (Mobile). And enters user name and password, if not previously saved, it connects to the AlsoRan Cloud Application Server. Auto login maybe enabled if the device is connected directly Mobile Anywhere facilities, Mobile and or Broadband, using other proxies (e.g. Single Sign On, Generic User profile (GUP), IMSI without a password).

4) The AlsoRan Cloud Application Server accesses it database and service profile for Mary.

5) The application displays a directory system of her file share system, showing Private and public directories and the files in each.

6) Mary transfers from her device memory a file to the client application.

7) Mary selects to move the file to the Private folder, the client application, communicates with AlsoRan Cloud Application Server to store a copy of the file.

8) AlsoRan Cloud Application Server communicates with McCloud that it is about to send a file for storage.

9) As the file is received by AlsoRan Cloud Application Server it is encrypted and sent to McCloud using information it received from McCloud on parameters and location of the infrastructure required to store the file.

10) On completions of the storage, Thunder-Cloud and McCloud provide a signal to AlsoRan Cloud Application Server that the file has been stored successfully and an indication is provided to Mary.

11) AlsoRan Cloud Application Server updates its database on the files it holds for Mary and their corresponding file descriptors in McCloud.

12) Mary selects another file, one with which she intends to commit an unlawful act and moves it to the Public folder.

13) The client uploads a copy of the file as described in steps 8 to 11.

14) AlsoRan Cloud Application Server then provides Mary with an FQDN to share the file with others.

15) Mary copies the file locator information and sends an SMS to an associate including the file locator information.

16) The associate Brad (who also is a subscriber of Mobile Anywhere) upon receipt of the SMS, copies the file locator to his client application, The AlsoRan Cloud Application Server forces Brad to log in. Once logged the Application Server request a file from McCloud that corresponds to the FQDN, decrypts it and sends it to Brad's client.

17) Mary selects a different device that has the file share application enabled.

18) Mary logs into the AlsoRan Cloud Application Server. The server determines that Mary is using a different device,

19) The AlsoRan Cloud Application Server accesses it database and service profile for Mary and determines that the File share Cloud service needs to sync with the service and from the data base, requests files to be down loaded from McCloud, decrypted and down loads one file to the local private director (mirror on the device) and one to the Public folder.

20) Sometime later Mary deletes the file from her shared folder (public).

21) Sometime later Mary will notice that all devices that are logged in to the File Share application will have their file removed from its local device memory.

22) A device that is not connected to the AlsoRan Cloud Application Server and not able to connect to the application will still retain a copy of the file until it is synchronized with the server.

Variation A

1 to 15 the same.

16) The associate Brad (who also is a subscriber of Mobile Anywhere) upon receipt of the SMS, forwards it to another associate Joan.

17) Joan connects to the internet and connects to the AlsoRan Cloud Application Server using the FQDN that identifies the file. The AlsoRan Cloud Application Server forces Joan to log in. Once logged the Application Server request a file from McCloud that corresponds to the FQDN, decrypts it and sends it to Joan's client.

18) Sometime later Mary deletes the file from her shared folder.

Variation B

1 to 15 the same.

16) The associate Brad (who also is a subscriber of Regional Mobile) upon receipt of the SMS, forwards it to another associate Gabor (who is not a subscriber of the Cloud Services).

17) Gabor connects to the internet and connects to the AlsoRan Cloud Application Server using the FQDN that identifies the file. The AlsoRan Cloud Application Server forces Gabor to log in. Login fails and Gabor is denied access to the file.

18) Sometime later Mary deletes the file from her shared folder.

Variation C

1 to 14 the same.

15) The client request Mary to enter in SMS and or email address of individuals to share the content. Their information is received by AlsoRan Cloud Application Server which then sends a unique messages to each recipient.

16) The associate Gabor upon receipt of the SMS or email, copies the message.

17) Gabor connects to the internet and connects to the AlsoRan Cloud Application Server using the FQDN that identifies the file.

18) AlsoRan Cloud Application Server checks the unique message against (non-exhaustive list, sms MSIDN, email address, log in credentials of the file share and) other server information to determine validly of the user accessing the file.

19) Upon successful validation delivers a copy of the decrypted file.

Variations to B and C

1) AlsoRan Cloud Application Server provides an indication when some has accessed the shared files.

2) Mary deletes the files from her shared folder.

e) Interaction with other services

1) The file Share may be part of an interactive Messaging platform, where all files are stored, voice mail, video mail and shared files.

2) It may be possible to access the shared folder via tele-prompts in the Messaging centre.

3) It may be possible to access the system via Web Browser client through the MNO's Web Portal.

4) It may be possible to delete files via Email commands sent to the server.

5) Local break with Femto cell and access to local shares and or use of Cellular Hub (cellular modem that terminates in wifi or Ethernet access) on Mary's personal network is for further study.

f) Roaming

1) When Mary roams to other networks, her File share travels with her and is accessible. Roaming Rates for data services may apply.

2) Mary can access the file share from local hotspots.

3) Mary could send a SMS or email to others with a file location to people not subscribers to Mobile Anywhere Cloud Service.

4) Local Break out services in the visited network is for further study.

g) Post Conditions

1) Mary and her associates Brad, Gabor and Joan have shared a file that has or will be used in an unlawful act.

2) Mary and the associates Brad, Gabor and Joan may have tried to hide any transactions.

3) The 3gpp-istan Police Department received the IRI and CC of Mary's communications. Using that information in their investigations, they prevent a crime from occurring.

4) Mobile Anywhere met their regulatory obligation to unobtrusively deliver communication to the authorized LEA.

h) Challenges for interception

1) Generally in the use case if a Warrant is effect at the time that Mary uploads the file, LEA should receive all related information.

2) It is not clear how attempts to access the file are communicated to LEA (FQDN access without login).

3) For specific implementations it is not clear if other means to delete the file can be captured.

4) It is not clear if Legal instruments are used in Inter-istan on McCloud, if they can stop access to specific files in 3gpp-istan (in this use case Mobile Anywhere has encrypted the data, thus obscuring the identity and the content of the files to determine any file to any user, however a court order could block access to all files (more a data retention issue, as real time delivery would be captured until the court order).

5) It is not clear how LEA will access the files in McCloud and or Thunder Cloud systems to preserve the contents of the file and its associated logs (business records, Data Storage).

6) How and what data/ IRI is presented to LEA (e.g. service type, clear text files, message deletions, message delivery (email)).

7) Various user identities used to access the files, IMSI, user name.

8) For specific implementations it is not clear how the Cloud Service "File share or Drop box" is communicated to LEA to identify the type of service the IRI and CC belong.

9) There may be multiple device attached and connected at the same time with the same or different identity (several web client, several mobile devices, PSTN connection via voice navigation, SMTP (email client)).

A.16 Consumer based File Sharing 6

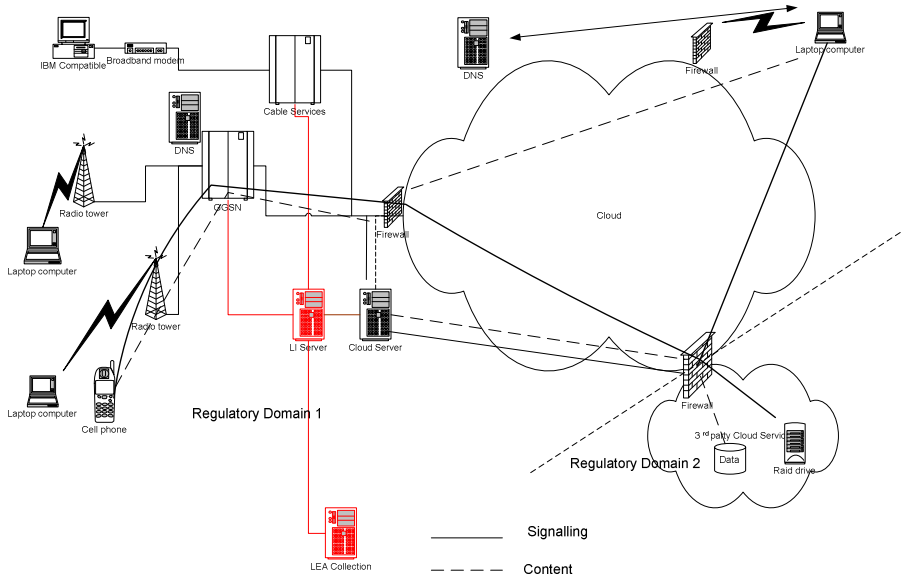


Figure A-7: MNO Cloud, File Share Proxy signalling, service in different Regulatory Domain

a) Overview

1) The MNO only allows access to File Sharing services only to subscribers of the service while on the MNO facilities or from Non 3GPP access networks.

a. The service can be offered with or without IMS services.

b) Actors

1) The user is Mary.

2) Brad is a user and an associate of Mary.

3) Joan is a user and an associate of Mary.

4) Joan has a subscription to the Cloud Service offered by Mobile Anywhere.

5) Gabor is an associate of Mary, Gabor does not have any affiliations with Mobile Anywhere.

6) Mobile Anywhere, is an MNO that provides access services on Mobile, fixed and broadband networks in the Domain of 3pp-istan.

7) AlsoRan is a vendor of 3GPP infrastructure.

8) Regional Mobile is a MNO that only allows mobile service in the Domain of 3pp-istan.

9) McCloud is a Cloud Service Provider in the Domain of Inter-istan.

10) Thunder-Cloud is a vendor or Cloud computing infrastructure in the Domain of Inter-istan.

c) Preconditions

1) Mary lives in 3pp-istan and is a subscriber Mobile Anywhere and has selected the File Sharing service. The service allows Mary to share files only between users and devices that have a subscription on Mobile Anywhere. A subscription is available to web access only subscribers not having any other services with Mobile Anywhere except the File Sharing service. The service does not provide encrypted services. The service is limited to 2 Gigabytes of storage. The use of the feature to move or retrieve files to or from the Cloud does not consume any access service plan. Mary can subscribe to larger storage plans.

2) Mobile Anywhere has contracted with McCloud to provide the service (File Sharing). Mobile Anywhere uses a Cloud Services Application from its Infrastructure Vendor AlsoRan. The Cloud Service Application can support many Cloud Services and provides Mobile Anywhere with integration interface to these services and the vendors that may be used to provide service.

3) AlsoRan provides a client that can operate on devices (smart phones, tablets and laptops) and the NNI, (Network to Network Interface) with McCloud. AlsoRan may hide the user's identity from McCloud.

4) McCloud does not manage access to shared files. Its client software provides a link address where the file is stored. Anyone with the link can access the file. Access to the File share system is via simple user name and password and can be stored in the client.

5) McCloud contracts with Thunder-Cloud to provide infrastructure to hosts it service. Thunder-Cloud and McCloud reside in Inter-istan.

6) Mobile Anywhere utilizes an FQDN to address the Cloud Service and redirects all requests to these File Share services to AlsoRan Cloud Service Application Server using its internal DNS server within Mobile Anywhere. External requests are directed to the appropriate Firewalls in Mobile Anywhere and to the Cloud Service Application Server.

7) The Cloud Service Application requires User logon in order to access the File Share application.

8) The Cloud Service Application may locally manage the subscriber information and store all users files as unique files as Mobile Anywhere files, hiding all users from McCloud.

9) Through the NII, several parameters may be utilized in Mobile Anywhere's deployment.

   a. Time to Live parameters, upon access of file

   b. Logon

   c. OAM Functionality

   d. Remote management of the service

   e. Access to files

   f. Access to unencrypted files

   g. Crypto keys to use

   h. Link Security.

   i. Quality of Service / Experience

10) McCloud maintains an NNI to Mobile Anywhere, it may maintain a data base of MNO and or of MNO and its Users. It may provide back up and restoration features.

11) McCloud and or Thunder-Cloud may protect the MNO and or User data.

12) AlsoRan may encrypt the files it stores with McCloud. These may be one key for all files or individual keys for each subscriber. Mobile Anywhere through AlsoRan manages these keys and are not provided to the subscriber.

d) Actions

1) The Mobile Anywhere surveillance facilities identify that a target of LI has initiated communication covered by the LI authorization and begins delivery of the communication to the LEA.

2) The 3gpp-istan Police Department begins receiving Mary's intercepted communications (i.e. IRI and CC for all required services as identified in the lawful authorization). The IRI and CC for the Consumer File Sharing service is delivered separately and the CC is the media that is sent to/from Mary (the Subject).

3) Mary selects the application from her device (Mobile). And enters user name and password, if not previously saved, it connects to the AlsoRan Cloud Application Server. Auto login maybe enabled if the device is connected directly Mobile Anywhere facilities, Mobile and or Broadband, using other proxies (e.g. Single Sign On, Generic User profile (GUP), IMSI without a password).

4) The AlsoRan Cloud Application Server accesses it database and service profile for Mary.

5) The AlsoRan Cloud Application Server contacts McCloud service, providing a token that identifies the user. McCloud responds with an FQDN that will providing the users file structure.

6) AlsoRan provides the FQDN to Mary's application.

7) The application displays a directory system of her file share system, showing Private and public directories and the files in each.

8) Mary transfers from her device memory a file to the client application.

9) Mary selects to move the file to the Private folder, the client application, communicates with McCloud Server to store a copy of the file.

10) McCloud Sever redirects Mary client to AlsoRan Cloud Application Server.

11) AlsoRan Cloud Application Server communicates with McCloud that it is about to send a file for storage, McCloud provides a link address.

12) If the file is to be encrypted by AlsoRan, it is received by AlsoRan Cloud Application Server it is encrypted and sent to McCloud using information it received from McCloud on parameters and location of the infrastructure required to store the file, if encryption is not to be used, AlsoRan Cloud Application Server, send Mary's Client the link it received from McCloud. IRI is generated, CC is generated if the file is to be encrypted.

13) On completions of the storage, Thunder-Cloud and McCloud provide a signal to AlsoRan Cloud Application Server that the file has been stored successfully and an indication is provided to Mary.

14) AlsoRan Cloud Application Server may update its database on the files it holds for Mary and their corresponding file descriptors in McCloud.

15) Mary selects another file, one with which she intends to commit an unlawful act and moves it to the Public folder.

16) The client uploads a copy of the file as described in steps 8 to 14.

17) AlsoRan Cloud Application Server then provides Mary with an FQDN to share the file with others.

18) Mary copies the file locator information and sends an SMS to an associate including the file locator information.

19) The associate Brad (who also is a subscriber of Mobile Anywhere) upon receipt of the SMS, copies the file locator to his client application, The AlsoRan Cloud Application Server forces Brad to log in. Once logged the Application Server request a location for the file from McCloud that corresponds to the FQDN, if the file is encrypted, the file is sent to AlsoRan Cloud Application Server, decrypted and sends it to Brad's client, if not encrypted, the file location is sent to Brad's client and the client then downloads the file from McCloud. IRI is generated, CC is generated if the file is to be encrypted.

20) Mary selects a different device that has the file share application enabled.

21) Mary logs into the AlsoRan Cloud Application Server. The server determines that Mary is using a different device.

22) The AlsoRan Cloud Application Server accesses it database and service profile for Mary and determines that the File share Cloud service needs to sync with the service and from the data base, requests files locations from McCloud, if the file is encrypted, the file is sent to AlsoRan Cloud Application Server, decrypted and sends it to Mary's client, if not encrypted, the file location is sent to Mary's client and the client then downloads the file from McCloud, one file to the local private director (mirror on the device) and one to the Public folder. IRI is generated, CC is generated if the file is encrypted.

23) Sometime later Mary deletes the file from her shared folder (public). Mary's client will send the delete command to AlsoRan Cloud Application Server which will send the command to McCloud. IRI is generated (note the file may be hidden for LEA purposes if so desired by proper commands).

24) Sometime later Mary will notice that all devices that are logged in to the File Share application will have their file removed from its local device memory (client messages not described). IRI is generated.

25) A device that is not connected to the AlsoRan Cloud Application Server and not able to connect to the application will still retain a copy of the file until it is synchronized with the server.

Variations A

1 to 18 the same.

19) The associate Brad (who also is a subscriber of Mobile Anywhere) upon receipt of the SMS, forwards it to another associate Joan.

20) Joan connects to the internet and connects to the AlsoRan Cloud Application Server using the FQDN that identifies the file. The AlsoRan Cloud Application Server forces Joan to log in. Once logged the Application Server request a file from McCloud that corresponds to the FQDN, if the file is encrypted, the file is sent to AlsoRan Cloud Application Server, decrypted and sends it to Joan's client, if not encrypted, the file location is sent to Joan's client and the client then downloads the file from McCloud, one file to the local private director (mirror on the device) and one to the Public folder. IRI is generated, CC is generated if the file is encrypted.

21) Sometime later Mary deletes the file from her shared folder.

Variation B

1 to 19 the same.

20) The associate Brad (who also is a subscriber of Regional Mobile) upon receipt of the SMS, forwards it to another associate Gabor (who is not a subscriber of the Cloud Services).

21) Gabor connects to the internet and connects to the AlsoRan Cloud Application Server using the FQDN that identifies the file. The AlsoRan Cloud Application Server forces Gabor to log in. Login fails and Gabor is denied access to the file.

22) Sometime later Mary deletes the file from her shared folder.

Variation C

1 to 16 the same.

17) The client request Mary to enter in SMS and or email address of individuals to share the content. Their information is received by AlsoRan Cloud Application Server which then sends a unique messages to each recipient.

18) The associate Gabor upon receipt of the SMS or email, copies the message.

19) Gabor connects to the internet and connects to the AlsoRan Cloud Application Server using the FQDN that identifies the file.

20) AlsoRan Cloud Application Server checks the unique message against (non-exhaustive list, sms MSIDN, email address, log in credentials of the file share and) other server information to determine validly of the user accessing the file.

21) Upon successful validation AlsoRan Cloud Application Sever request McCloud to provide a file location for the FQDN, if the file is encrypted, the file is sent to AlsoRan Cloud Application Server, decrypted and sent it to Gabor's client, if not encrypted, the file location is sent to Gabor's client and the client then downloads the file from McCloud. IRI is generated, CC is generated if the file is encrypted. Mobile anywhere insists on a time to live is associated with the file location and if the client does not retrieve the file in time it tries again and if a user snoops into the IP and obtains the file locations, it will have expired before it can be used and will result in an error message.

Variations to B and C

1) AlsoRan Cloud Application Server and or McCloud via AlsoRan Cloud application Server provides an indication when some has accessed the shared files.

2) Mary deletes the files from her shared folder.

e) Interaction with other services

1) The file Share may be part of an interactive Messaging platform, where all files are stored, voice mail, video mail and shared files.

2) It may be possible to access the shared folder via tele-prompts in the Messaging centre.

3) It is possible to access the system via Web Browser client through the MNO's Web Portal.

4) It may be possible to delete files via Email commands sent to the server.

5) Local break with Femto cell and access to local shares and or use of Cellular Hub (cellular modem that terminates in wifi or Ethernet access) on Mary's personal network is for further study

f) Roaming

1) When Mary roams to other networks, her File share travels with her and is accessible. Roaming Rates for data services may apply.

2) Mary can access the file share from local hotspots.

3) Mary could send a SMS or email to others with a file location to people not subscribers to Mobile Anywhere Cloud Service.

4) Local Break out services in the visited network is for further study.

g) Post Conditions

1) Mary and her associates Brad, Gabor and Joan have shared a file that has or will be used in an unlawful act.

2) Mary and the associates Brad, Gabor and Joan may have tried to hide any transactions

3) The 3gpp-istan Police Department received the IRI and some CC of Mary's communications. The actual contents of Mary files may be missing if not encrypted by the MNO and other means will be required to capture that content. Using that information in their investigations, they may be able to prevent a crime from occurring.

4) Mobile Anywhere may have met their regulatory obligation to unobtrusively deliver communication to the authorized LEA.

h) Challenges for interception

1) Generally in the use case if a Warrant is effect at the time that Mary uploads the file, LEA should receive all related IRI information.

2) It is not clear how attempts to access the file are communicated to LEA (FQDN access without login).

3) For specific implementations it is not clear if other means to delete the file can be captured.

4) It is not clear if Legal instruments are used in Inter-istan on McCloud, if they can stop access to specific files in 3gpp-istan (in this use case Mobile Anywhere has encrypted the data, thus obscuring the identity and the content of the files to determine any file to any user, however a court order could block access to all files (more a data retention issue, as real time delivery would be captured until the court order).

5) It is not clear how LEA will access the files in McCloud and or Thunder Cloud systems to preserve the contents of the file and its associated logs (business records, Data Storage).

6) How and what data/ IRI is presented to LEA (e.g. service type, clear text files, message deletions, message delivery (email)).

7) Various user identities used to access the files, IMSI, user name.

8) For specific implementations it is not clear how the Cloud Service "File share or Drop box" is communicated to LEA to identify the type of service the IRI and CC belong.

9) There may be multiple device attached and connected at the same time with the same or different identity (several web client, several mobile devices, PSTN connection via voice navigation, SMTP (email client))

10) Type of message and associate information to be use if the Time to live parameter is exceed in a legitimate attempt and one that is an illegal attempt.

A.17 Consumer based File Sharing 7

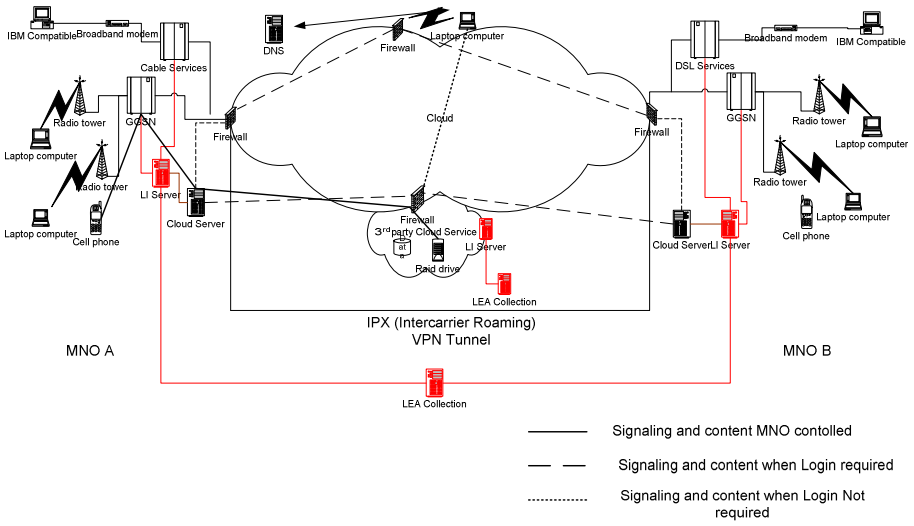


Figure A-8: Small Medium Business with multiple MNO

a) Overview

1) The SMB and or Enterprise require two or more MNOs to provide its Cloud service for file sharing for their employees. The MNO have white labelled a service from the same Cloud provider.

a. The service can be offered with or without IMS services.

b) Actors

1) The user is John.

2) Joan is a user and an associate of John.

3) Brad is a user and an associate of John.

4) Mobile Anywhere is an MNO that provides access services on Mobile, fixed and broadband networks in the Domain of 3gpp-istan.

5) Regional Mobile is a MNO that only allows mobile service in the Domain of 3gpp-istan.

6) Jungle Cloud is a Cloud Service Provider in the Domain of 3gpp-istan.

7) Hyper-Cloud is a vendor or Cloud computing infrastructure in the Domain of 3gpp-istan.

c) Preconditions

1) John, Joan and Brad live in 3gpp-istan and work for a Small national Business company that have farmed out their IT infrastructure and use a Bring your own Device (BYOD) model for their employees, which includes laptops, PC and wireless devices for access to the company files, email and subscriber databases. The SMB has chosen to place all it files and databases on Cloud infrastructure and has negotiated with the MNO in 3gpp-istan to provide access for their employees using their mobile, wifi and broadband connections.

2) Regional Mobile and Mobile Anywhere have white labelled a service from Jungle Cloud which in turn uses Hyper-Cloud infrastructure. Each MNO may tweak the service it provides, but a Jungle Cloud client is provided to each user that is labelled with the MNO offering. The Cloud service requires Login and passwords that are stored in Jungle Cloud. The service provides private directories for users, shared directories and public directories. Access to each is controlled by permissions allocated by the IT group of the SMB.

3) The service allows all to access files only between users and devices that have a subscription on Jungle Cloud and a member of the folders. A subscription is available to web access only subscribers not having any other services. The service does not provide encrypted files services. But it uses SSL on web access and VPN tunnels to the MNO's infrastructure.

   Assumed that the MNO know their legal obligation for access and have requested VPN so that the files are in the clear when delivered over their networks, which are encrypted from others and encrypted over public access facilities.

4) A support function is provided by the MNO's via Jungle Cloud to add/modify/delete users from the file share and to added other directories and permissions. A separate archival service is available.

5) Jungle Cloud provides a client to the MNO that can be White labelled that can operate on devices (smart phones, tablets and laptops).

6) Jungle Cloud manages access to shared files. Its client software provides a link address where the file is stored. Anyone with the link can access the file if they have logged in and have permission for that directory. Access to the File share system is via simple user name and password and can be stored in the client.

7) Jungle Cloud contracts with Hyper-Cloud to provide infrastructure to hosts it service.

8) Jungle Cloud or Hyper-Cloud may have Dynamic triggering capabilities.

9) The Jungle Cloud Client utilizes an FQDN to address the Cloud Service. All requests in the MNO are directed to the VPN to Jungle Cloud Service. External requests are directed via DNS directly to Jungle Cloud.

10) The Cloud Service Application requires User logon in order to access the File Share application.

11) The Cloud Service Application may locally manage the subscriber information and store all users' files as unique files associated with the users or as SMB files. It may encrypt that files that are stored on the Cloud to protect access from others, but delivers the files in clear text which is then encrypted for the access (VPN or SSL).

12) Through agreements, several parameters may be utilized in deployment.

    a. Time to Live parameters, upon access of file

    b. Logon

    c. OAM Functionality

    d. Remote management of the service

    e. Access to files

    f. Access to unencrypted files

    g. Crypto keys to use

    h. Link Security

    i. Quality of Service / Experience

13) The MNO's may have an NNI to Jungle Cloud.

14) The SMB may encrypt the files it stores with the MNO. These may be one key for all files or individual keys for each subscriber using open PGP software.

d) Actions

1) John is the target of a legal warrant.

2) Regional Mobile surveillance facilities identify that a target of LI has initiated communication covered by the LI authorization and begins delivery of the communication to the LEA.

3) The 3gpp-istan Police Department begins receiving John's intercepted communications (i.e. IRI and CC for all required services as identified in the lawful authorization). The IRI and CC for the File Sharing service is delivered separately and the CC is the media that is sent to/from John (the Subject).

4) John selects the application from his device (Mobile). And enters user name and password, if not previously saved, it connects to the Jungle Cloud -Cloud Application Server. Auto login maybe enabled if the device is connected directly Regional Mobile facilities, using other proxies (e.g. Single Sign On, Generic User profile (GUP), IMSI without a password).

5) The Jungle Cloud accesses it database and service profile for John and the associated SMB.

6) Jungle Cloud responds with an FQDN that will provide the users file structure.

7) The application displays a directory system of his directories that he has access, showing his Private, SMB shared and public directories and the files in each.

8) John transfers from his device memory a file to the client application.

9) John selects to move the file to the SMB Shared folder, the client application, communicates with Jungle Cloud Server to store a copy of the file.

10) Jungle Cloud provides a link address.

11) On completions of the storage, Jungle-Cloud provide an indication is provided to John.

12) During this time IRI is generated, CC is generated.

13) John selects another file, one with which he intends to commit an unlawful act and moves it to the Public folder.

14) The client uploads a copy of the file as described in steps 8 to 12.

15) Jungle Cloud Server then provides John with an FQDN to share the file with others.

16) John copies the file locator information and sends an SMS to an associate including the file locator information. IRI is generated. This could be used in Dynamic Triggering to set up other cooperating systems for associates. Dynamic triggers will not be effective if the user writes down the file location unless the triggering is based on the file itself.

17) The associate Brad (who also is a subscriber of Mobile Anywhere) upon receipt of the SMS, copies the file locator to his client application and the client then downloads the file from Jungle Cloud. No IRI is generated, nor CC as Brad is not the subject of the interception. If a Warrant were placed on Mobile Anywhere for Brad then IRI and CC would be generated. If a warrant were placed at Jungle Cloud then IRI and CC would be generated. Information collected from each entity may be different, Jungle Cloud could provide additional detail not available from Mobile Anywhere and Regional Mobile, but cannot provide location precision that the MNO can provide.

18) John selects a different device that has the file share application enabled.

19) John logs into the Jungle Cloud Server using a Hotspot connection with his laptop. The server determines that John is using a different device.

20) The Jungle Cloud Server accesses it database and service profile for John and determines that the File share Cloud service needs to sync with the service. Several files are downloaded to John's device. No IRI is generated, no CC is generated.

21) Sometime later John deletes the file from the Public folder. John's client will send the delete command to Jungle Cloud Server. No IRI is generated. The file may be retained for legal, financial, archival (Business Continuity), restoral purposes as determined by the SMB Service Contracts, MNO needs or by Jungle Cloud).

22) Sometime later John will notice that all devices that are logged in to the File Share application will have their file removed from its local device memory. (Client messages not described) IRI is generated only when John Mobile device is active. The deleted files may be accessible by file recovery programs.

23) A device that is not connected to the Jungle Cloud Server and not able to connect to the application will still retain a copy of the file until it is synchronized with the server.

Variation A

1 to 16 the same.

17) The associate Brad (who also is a subscriber of Mobile Anywhere) upon receipt of the SMS, forwards it to another associate Joan.

18) Joan connects to the internet and connects to the Jungle Cloud Server using the FQDN that identifies the file. The Jungle Cloud Server delivers the file from the Public folder. No IRI is generated, no CC is generated.

19) Sometime later John deletes the file from the Public folder.

Variations to A

1) Jungle Cloud Server provides an indication when some has accessed the Public Folder to the SMB.

2) Someone else in the SMB deletes the files from the Public folder.

e) Interaction with other services

1) The file Share may be part of an interactive Messaging platform, where all files are stored, voice mail, video mail and shared files.

2) It may be possible to access the shared folder via tele-prompts in the Messaging centre.

3) It is possible to access the system via Web Browser client through the MNO's Web Portal.

4) It may be possible to delete files via Email commands sent to the server.

5) Local break with Femto cell and access to local shares and or use of Cellular Hub (cellular modem that terminates in Wi-Fi or Ethernet access) on John's personal network is for further study.

f) Roaming

1) When John roams to other networks, his File share travels with him and is accessible. Roaming Rates for data services may apply.

2) John can access the file share from local hotspots.

3) John could send a SMS or email to others with a file location to people not subscribers to Mobile Anywhere Cloud Service.

4) Local Break out services in the visited network is for further study.

g) Post Conditions

1) John and her associates Brad and Joan have shared a file that has or will be used in an unlawful act.

2) John and the associates Brad and Joan may have tried to hide any transactions.

3) The 3gpp-istan Police Department received the IRI and some CC of John's communications via Regional Mobile when John was using his mobile device. The communication on other service (Hotspot or Broadband) were not captured and other means will be required to capture that content and IRI. Using that information in their investigations, they may be able to prevent a crime from occurring.

4) Regional Mobile has met their regulatory obligation to unobtrusively deliver communication to the authorized LEA.

h) Challenges for interception

1) Generally in the use case if a Warrant is effect at the time that John uploads the file, LEA should receive all related IRI information from that Service provider.

2) It is clear that other warrants are required to capture other events while at a hotspot or on a broadband connection.

3) For specific implementations it is not clear if other means to delete the file can be captured.

4) It is not clear what interface will be used by Jungle Cloud if they were served a Warrant. Some aspect of messaging, data retention and data in motion exist.

5) It is not clear how LEA will access the files in Jungle Cloud systems to preserve the contents of the file and its associated logs (business records, Data Storage).

6) How and what data/ IRI is presented to LEA (e.g. service type, clear text files, message deletions, message delivery (email)).

7) Various user identities used to access the files, IMSI, user name, HTTP identity.

8) For specific implementations it is not clear how the Cloud Service "Private, Shared, Public" is communicated to LEA to identify the type of service the IRI and CC belong.

9) There may be multiple device attached and connected at the same time with the same or different identity (several web client, several mobile devices, PSTN connection via voice navigation, SMTP (email client)). If captured at Jungle Cloud, if several devices are logged in and the user up loads a file, all devices will by synced cause duplication of all the CC.

10) It is unclear what would be captured on the NNI interfaces, i.e. if permissions for John were changed.

A.18 Consumer based File Sharing 8

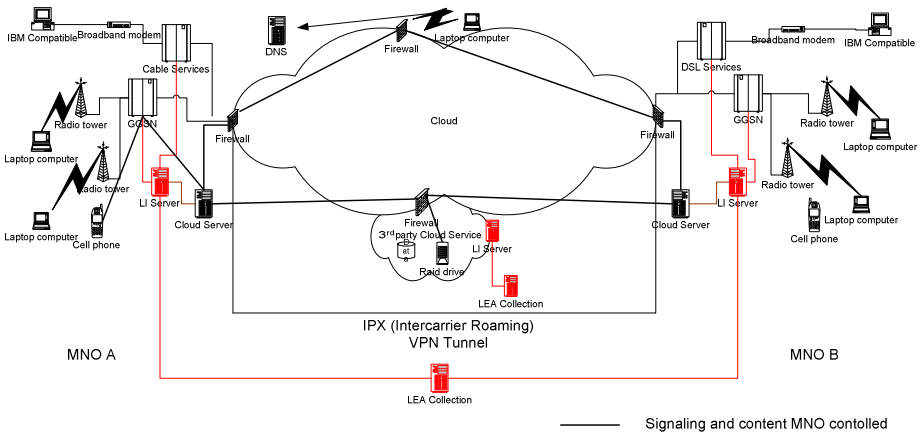


Figure A-9

a) Overview

1) The SMB and or Enterprise require two or more MNOs to provide its Cloud service for file sharing for their employees. The MNO have white labelled a service from the same Cloud provider.

a. The service can be offered with or without IMS services.

b) Actors

1) The user is John.

2) Joan is a user and an associate of John.

3) Brad is a user and an associate of John.

4) Mobile Anywhere is an MNO that provides access services on Mobile, fixed and broadband networks in the Domain of 3pp-istan.

5) Regional Mobile is a MNO that only allows mobile service in the Domain of 3gpp-istan.

6) Jungle Cloud is a Cloud Service Provider in the Domain of 3gpp-istan.

7) Hyper-Cloud is a vendor or Cloud computing infrastructure in the Domain of 3gpp-istan.

c) Preconditions

1) John, Joan and Brad live in 3pp-istan and work for a Small national Business company that have farmed out their IT infrastructure and use a Bring your own Device (BYOD) model for their employees, which includes laptops, PC and wireless devices for access to the company files, email and subscriber databases. The SMB has chosen to place all it files and databases on Cloud infrastructure and has negotiated with the MNO in 3gpp-istan to provide access for their employees using their mobile, wifi and broadband connections.

2) Regional Mobile and Mobile Anywhere have white labelled a service from Jungle Cloud which in turn uses Hyper-Cloud infrastructure. Each MNO provides an AlsoRan Proxy Cloud Server in their networks to interface to Jungle Cloud. Each MNO may tweak the service it provides, but an AlsoRan client is provided to each user that is labelled with the MNO offering. The service provides private directories for users, shared directories and public directories. Access to each is controlled by permissions allocated by the IT group of the SMB.

3) AlsoRan provides a client that can operate on devices (smart phones, tablets and laptops) and the NNI, (Network to Network Interface) with Jungle Cloud. AlsoRan may hide the user's identity from Jungle Cloud.

4) Jungle Cloud does not manage access to shared files. Its client software provides a link address where the file is stored. Anyone with the link can access the file. Access to the File share system is via simple user name and password and can be stored in the client.

5) The service allows all to access files only between users and devices that have a subscription with the MNO and are members of the folders. A subscription is available to web access only subscribers not having any other services. The service does not provide encrypted files services. But it uses SSL on web access and VPN tunnels to the MNO's infrastructure.

   Assumed that the MNO know their legal obligation for access and have requested VPN so that the files are in the clear when delivered over their networks, which are encrypted from others and encrypted over public access facilities.

6) A support function is provided by the MNO's via Jungle Cloud to add/ modify / delete users from the file share and to added other directories and permissions. A separate archival service is available.

7) Jungle Cloud contracts with Hyper-Cloud to provide infrastructure to hosts it service.

8) Jungle Cloud or Hyper-Cloud may have Dynamic triggering capabilities.

9) The AlsoRan Client utilizes an FQDN to address the Cloud Service. All requests in the MNO are directed to the VPN to Jungle Cloud Service via the Proxy Cloud Sever. External requests are directed via DNS to the appropriate MNO that supports the user access to Public folders, from Broadband, these can split between the MNOs or directed to Jungle Cloud and it makes a decision on routing of addresses via the MNO or it is not addressed by the MNO.

10) The Cloud Service Application requires User logon in order to access the File Share application.

11) The Cloud Service Application may locally manage the subscriber information and store all users' files as unique files associated with the users or as SMB files. It may encrypt that files that are stored on the Cloud to protect access from others, but delivers the files in clear text which is then encrypted for the access (VPN or SSL).

12) Through agreements, several parameters may be utilized in deployment.

    a. Time to Live parameters, upon access of file

    b. Logon

    c. OAM Functionality

    d. Remote management of the service

    e. Access to files

    f. Access to unencrypted files

    g. Crypto keys to use

    h. Link Security

    i. Quality of Service / Experience

13) The MNO's may have an NNI to Jungle Cloud.

14) Jungle Cloud may maintain a data base of MNO and or of MNO and its Users. It may provide back up and restoration features.

15) Jungle Cloud and or Hyper-Cloud may protect the MNO and or User data.

16) AlsoRan may encrypt the files it stores with Jungle Cloud. These may be one key for all files or individual keys for each subscriber. Mobile anywhere and Regional Mobile may use a common encryption service (Media Security)) to manages these keys and are not provided to the subscriber.

17) The SMB may encrypt the files it stores with the MNO. These may be one key for all files or individual keys for each subscriber using open PGP software.

d) Actions

1) John is the target of a legal warrant.

2) Regional Mobile surveillance facilities identify that a target of LI has initiated communication covered by the LI authorization and begins delivery of the communication to the LEA.

3) The 3gpp-istan Police Department begins receiving John's intercepted communications (i.e. IRI and CC for all required services as identified in the lawful authorization). The IRI and CC for the File Sharing service is delivered separately and the CC is the media that is sent to/from John (the Subject).

4) John selects the application from his device (Mobile). And enters user name and password, if not previously saved, it connects to the AlsoRan Cloud Application Server. Auto login maybe enabled if the device is connected directly Regional Mobile facilities, using other proxies (e.g. Single Sign On, Generic User profile (GUP), IMSI without a password).

5) The AlsoRan Cloud Application Server accesses it database and service profile for John and the associated SMB.

6) The application displays a directory system of his file share system, Personal, SMB Private and public directories and the files in each that John has access.

7) John transfers from his device memory a file to the client application.

8) John selects to move the file to the SMB Private folder, the client application, communicates with AlsoRan Cloud Application Server to store a copy of the file.

9) AlsoRan Cloud Application Server communicates with Jungle Cloud that it is about to send a file for storage.

10) The AlsoRan Cloud server in Regional Mobile communicates with a key server to retrieve the common key used by the SMB.

11) As the file is received by AlsoRan Cloud Application Server it is encrypted and sent to Jungle Cloud using information it received from Jungle Cloud on parameters and location of the infrastructure required to store the file.

12) On completions of the storage, Hyper-Cloud and Jungle Cloud provide a signal to AlsoRan Cloud Application Server that the file has been stored successfully and an indication is provided to John.

13) AlsoRan Cloud Application Server updates its database on the files it holds for John and their corresponding file descriptors in Jungle Cloud.

14) During this time IRI is generated, CC is generated.

15) John selects another file, one with which he intends to commit an unlawful act and moves it to the Public folder.

16) The client uploads a copy of the file as described in steps 8 to 14.

17) AlsoRan Server then provides John with an FQDN to share the file with others.

18) John copies the file locator information and sends an SMS to an associate including the file locator information. IRI is generated. This could be used in Dynamic Triggering to set up other cooperating systems. Dynamic triggers will not be effective if the user writes down the file location unless the triggering is based on the file itself.

19) The associate Brad (who also is a subscriber of Mobile Anywhere) upon receipt of the SMS, copies the file locator to his client application, the file is located in the Regional Mobile and that AlsoRan Cloud Application Server forces Brad to log in. Once logged the Application Server request a file from Jungle Cloud that corresponds to the FQDN, a key for the SMB from a key server and then decrypts it and sends it to Brad's client. It may be possible that the URI used in the SMS, email can be parsed by a client to a different network, i.e. Brad client could have replaced the Regional Mobile (www.regionalmobile.3gppistan/Cloud/smb/index=? 12345678qwededed) with corresponding Mobile Anywhere prefixes to address the same file location that would be in Jungle Cloud. In this case LI information may not be captured unless other processes occur. The MNO could map APN information to provide a similar function and VPN tunnel between MNO for the Cloud sharing service resolving the DNS query to Regional Mobile, thus Brad clients would access the VPN tunnel and show up in Regional Mobiles AlsoRan Cloud Server. User name/ Passwords authentication is possible via VPN tunnels between the MNO and the Proxy servers.

20) John selects a different device that has the file share application enabled.

21) John logs into the AlsoRan Cloud Server using a Hotspot connection with his laptop. The server determines that John is using a different device.

22) The AlsoRan Cloud Application Server accesses it database and service profile for John and determines that the Files and directories for the SMB Cloud service needs to sync with the service and from the data base, requests files to be down loaded from Jungle Cloud, a key for the SMB from a key server and then decrypts and several files are downloaded to Johns device. IRI is generated, CC is generated.

23) Sometime later John deletes the file from the Public folder. John's client will send the delete command to AlsoRan Cloud Server (client messages not described to Jungle Cloud). IRI is generated. The file may be retained for legal, financial, archival (Business Continuity), restoral purposes as determined by the SMB Service Contracts, MNO needs or by Jungle Cloud).

24) Sometime later John will notice that all devices that are logged in to the File Share application will have their file removed from its local device memory. (Client messages not described) IRI is generated for all of John active devices. The deleted files may be accessible by file recovery programs.

25) A device that is not connected to the Jungle Cloud Server and not able to connect to the application will still retain a copy of the file until it is synchronized with the server.

Variation A

1 to 18 the same.

19) The associate Brad (who also is a subscriber of Mobile Anywhere) upon receipt of the SMS, forwards it to another associate Joan.

20) Joan connects to the internet and connects to the AlsoRan Cloud Application Server using the FQDN that identifies the file. The AlsoRan Cloud Application Server forces Joan to log in. Once logged the Application Server request a file from Jungle Cloud that corresponds to the FQDN, a key for the SMB from a key server and then decrypts it and sends it to Joan's client.

21) Sometime later John deletes the file from the Public folder.

Variation B

1 to 18 the same.

19) The associate Brad (who also is a subscriber of Regional Mobile) upon receipt of the SMS, forwards it to another associate Gabor (who is not a subscriber of the Cloud Services).

20) Gabor connects to the internet and connects to the AlsoRan Cloud Application Server using the FQDN that identifies the file. The AlsoRan Cloud Application Server forces Gabor to log in. Login fails and Gabor is denied access to the file.

21) Sometime later John deletes the file from the Public folder.

Variations C

1 to 17 the same.

18) The client request John to enter in SMS and or email address of individuals to share the content. Their information is received by AlsoRan Cloud Application Server which then sends a unique messages to each recipient.

19) The associate Gabor upon receipt of the SMS or email, copies the message.

20) Gabor connects to the internet and connects to the AlsoRan Cloud Application Server using the FQDN that identifies the file.

21) AlsoRan Cloud Application Server checks the unique message against (non-exhaustive list, sms MSIDN, email address, log in credentials of the file share and) other server information to determine validly of the user accessing the file.

22) Upon successful validation delivers a copy of the decrypted file.

Variations to B and C

1) AlsoRan Cloud Application Server provides an indication when some has accessed the shared files.

2) Someone else in the SMB deletes the files from the Public folder.

e) Interaction with other services

1) The file Share may be part of an interactive Messaging platform, where all files are stored, voice mail, video mail and shared files.

2) It may be possible to access the shared folder via tele-prompts in the Messaging centre.

3) It is possible to access the system via Web Browser client through the MNO's Web Portal.

4) It may be possible to delete files via Email commands sent to the server.

5) Local break with Femto cell and access to local shares and or use of Cellular Hub (cellular modem that terminates in wifi or Ethernet access) on John's personal network is for further study.

f) Roaming

1) When John roams to other networks, his File share travels with him and is accessible. Roaming Rates for data services may apply.

2) John can access the file share from local hotspots.

3) John could send a SMS or email to others with a file location to people not subscribers to Mobile Anywhere Cloud Service.

4) Local Break out services in the visited network is for further study.

g) Post Conditions

1) John and his associates Brad and Joan have shared a file that has or will be used in an unlawful act.

2) John and the associates Brad and Joan may have tried to hide any transactions.

3) The 3gpp-istan Police Department received the IRI and CC of John's communications. By using that information in their investigations, they prevent a crime from occurring.

4) Regional Mobile met their regulatory obligation to unobtrusively deliver communication to the authorized LEA.

h) Challenges for interception

1) Generally in the use case if a Warrant is effect at the time that John uploads the file, LEA should receive all related IRI information from that Service provider.

2) It is clear that other warrants are required to capture other events while at a hotspot or on a broadband connection.

3) For specific implementations it is not clear if other means to delete the file can be captured.

4) It is not clear how LEA will access the files in Jungle Cloud systems to preserve the contents of the file and its associated logs (business records, Data Storage).

5) How and what data/ IRI is presented to LEA (e.g. service type, clear text files, message deletions, message delivery (email)).

6) Various user identities used to access the files, IMSI, user name, HTTP identity.

7) For specific implementations it is not clear how the Cloud Service "Private, Shared, Public" is communicated to LEA to identify the type of service the IRI and CC belong.

8) There may be multiple device attached and connected at the same time with the same or different identity (several web client, several mobile devices, PSTN connection via voice navigation, SMTP (email client)).

9) It is unclear what would be captured on the NNI interfaces, i.e. if permissions for John were changed.

A.19 Access Network Discovery and Selection Function (ANDSF) Use Case

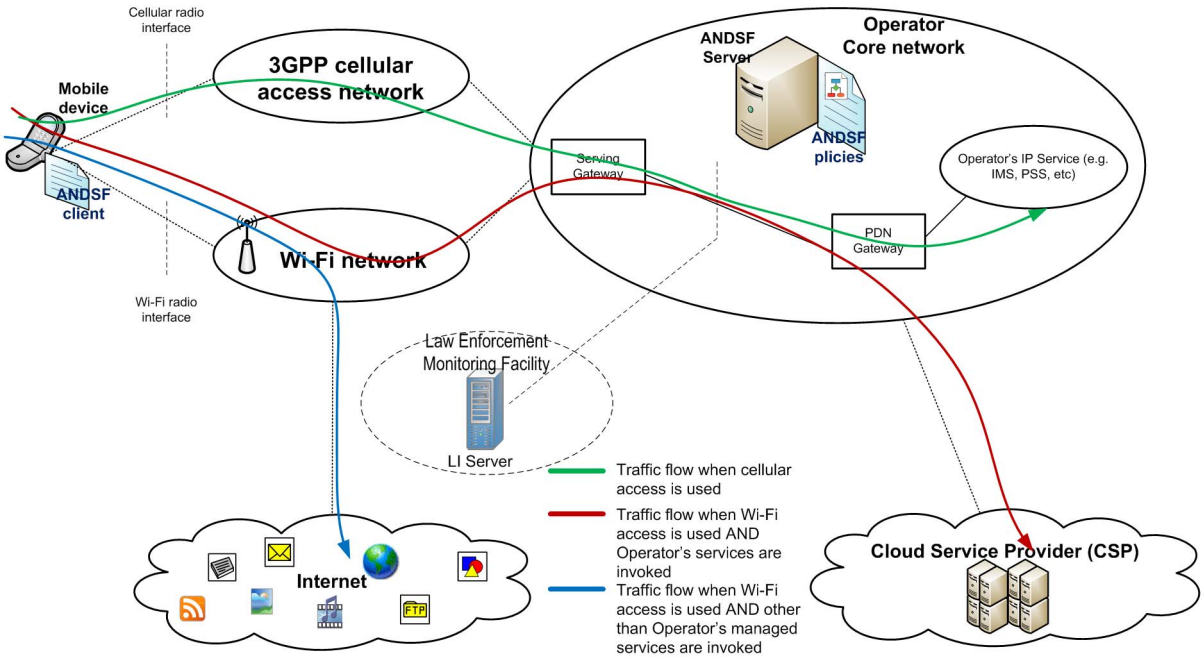


Figure A-10: Use of ANDSF with Operator provided Cloud Services

a) Overview

1) The MNO only allows File sharing services that control by a policy server (ANDSF) to subscribers on its and Non 3GPP access networks.

a. The Cloud Facilities are external to the MNO domain but only accessible via the MNO.

b. The service can be offered with or without IMS services.

b) Actors

1) The user is John.

2) Mobile Anywhere is a Mobile Network Operator (MNO).

3) McCloud is a Cloud Service Provider (CSP).

c) Preconditions

1) John is a subscriber to a mobile data service from Mobile Anywhere. John has a subscription to a Cloud service, type of DaaS - Data as a Service (e.g. data storage in the Cloud) from Mobile Anywhere. There is a business relationship between Mobile Anywhere and McCloud such as that McCloud provides 'White-labelled' Cloud services to Mobile Anywhere.

2) John carries a UE that has WLAN capabilities (i.e. dual mode handset, Wi-Fi + cellular) and an installed ANDSF client.

3) Mobile Anywhere operates an ANDSF Server in its network. The server is under its full control and provides policies that could be used by the mobile device regarding:

a. Access network discovery

b. ISMP (Inter System Mobility Policy)

c. ISRP (Inter System Routing Policy)

4) Mobile Anywhere can provision John's UE with its policies by using the ANDSF mechanism.

5) John's UE has an ANDSF client that can connect securely with the ANDSF server to get periodical updates, which may change based on John's location, time of day or other attributes.

6) Mobile Anywhere can configure a list of its managed services and their associated routing policies, e.g.:

   a. Cloud Services -- traffic is routed through core network

   b. VoIP - traffic is routed through core network

   c. Other services (e.g. web browsing) -- may not be routed through core network

7) UE is configured with enhanced operator's policies to enable rules to route traffic for different applications between the Wi-Fi and cellular networks in general and may invoke policies in case of Lawful Intercept.

d) Actions

1) The Mobile Anywhere surveillance facilities identify that a target of LI has initiated communication covered by the LI authorization and begins delivery of the communication to the LEA.

2) The 3gpp-istan Police Department begins receiving John's intercepted communications (i.e. IRI and CC for all required services as identified in the lawful authorization). The IRI and CC for the File Sharing service is delivered separately and the CC is the media that is sent to/from John's (the Subject).

3) John connects his UE to an available Wi-Fi network.

4) John, as a subscriber of Cloud service, decides to retrieve a file from his Cloud service account.

5) Based on the Mobile Anywhere's policies provisioned in the UE, John's traffic leaving Wi-Fi network is routed through operator's core network, instead of going directly to the internet and access to the Cloud service occurs.

6) The file requested from the Cloud service passes through Mobile Anywhere's Network and is delivered to John's UE.

7) During this time IRI is generated, CC is generated.

e) Interaction with other services

1) Other application on johns UE may have polies set by the ANSDF to egress through the hotspot to the public internet and are not passed to Mobile Anywhere.

2) Local break with Femto cell and access to local shares and or use of Cellular Hub (cellular modem that terminates in Wi-Fi or Ethernet access) on John's personal network is for further study.

f) Roaming

1) When John roams to other networks, his DaaS service travels with him and is accessible. Roaming Rates for data services may apply.

2) John can access the file from local hotspots.

3) Local Break out services in the visited network is for further study.

g) Post-conditions

1) John was the subject of legal interception and he accessed a file from his Cloud service.

2) Mobile Anywhere's is able to intercept John's file while transiting Mobile Anywhere's network, through the use of its ANDSF policy server and UE client application.

3) The 3gpp-istan Police Department received the IRI and CC of John's communications. Using that information in their investigations, they prevent a crime from occurring.

4) Mobile Anywhere met their regulatory obligation to unobtrusively deliver communication to the authorized LEA.

Annex B:
Cloud Virtualization Fora

Abbreviation	Forum Name	SubGroup	SubGroup Name	SubGroup URL
Cloud industry platform technical standards developer forums				
Android	Android Developers Forum			http://developer.android.com/index.html
AWS	Amazon Web Services Forum			https://forums.aws.amazon.com/forum.jspa?forumID=30
BMC	BMC Software			http://www.bmc.com/solutions/Cloud-computing/Cloud-computing-management/Cloud-Computing-Management-CCM.html
CA	CA Technologies			http://www.ca.com/us/Cloud-solutions.aspx
Cisco	Cisco Developer Network			http://developer.cisco.com/web/partner/search?technologyIds=a0G400000070wGiEAI
	CloudMade			http://cloudmade.com/
	GitHub			https://github.com/
Google	Google Developers			https://developers.google.com/
HP	HP Cloud Services			https://hpcloud.com/content/about-us
IBM	developerWorks			http://www.ibm.com/developerworks/aboutdw/contacts.html
iCloud	iCloud for Developers			https://developer.apple.com/icloud/index.php
Intel	Intel Cloud Builders			http://www.intel.com/content/www/us/en/Cloud-computing/Cloud-builders-provide-proven-advice.html?cid=sem116p9128
Jive	Jive apps developers			https://developers.jivesoftware.com/community/index.jspa
Microsoft	Windows Azure Community			http://www.windowsazure.com/en-us/community/blog/
Oracle	Oracle Cloud Computing			http://www.oracle.com/us/technologies/Cloud/index.html
	ProgrammableWeb			http://www.programmableweb.com/
Radckspace	OpenStack Developer Community			http://www.rackspace.com/blog/
RedHat	OpenShift Developer Community			https://openshift.redhat.com/app/platform
	SourceForge			http://sourceforge.net/
	TopCoder			http://www.topcoder.com/

Abbreviation	Forum Name	SubGroup	SubGroup Name	SubGroup URL
VMware	VMware Community		[multiple]	http://communities.vmware.com/groups/
xda	XDA Developers Forum			http://forum.xda-developers.com/
Cloud industry generic technical standards forums				
3GPP	3rd Generation Partnership Project	CT1	MM/CC/SM [lu]	http://portal.etsi.org/portal/server.pt/community/3GPP/296?tbId=651
3GPP	3rd Generation Partnership Project	SA2	Architecture	http://portal.etsi.org/portal/server.pt/community/3GPP/296?tbId=385
3GPP	3rd Generation Partnership Project	SA3	Security	http://portal.etsi.org/portal/server.pt/community/3GPP/296?tbId=386
3GPP	3rd Generation Partnership Project	SA3LI	Mobile LI	http://portal.etsi.org/portal/server.pt/community/3GPP/296?tbId=386
ARTS	Association for Retail Technology Standards		UnifiedPOS	http://www.nrf-arts.org/
ARTS	Association for Retail Technology Standards		Data Model	http://www.nrf-arts.org/
ARTS	Association for Retail Technology Standards		ARTS XML	http://www.nrf-arts.org/
ARTS	Association for Retail Technology Standards		Standard RFPs	http://www.nrf-arts.org/
ATIS	Alliance for Telecommunications Industry Solutions	SON	Service Oriented Network Forum	http://www.atis.org/SON/index.asp
CA/B Forum	Certification Authority Browser Forum			http://www.cabforum.org/
CableLabs	CableLabs			http://www.cablelabs.com/
CCDB	Common Criteria Control Board			http://www.commoncriteriaportal.org/cc/
CCDB	Common Criteria Control Board	CC Forum	Common Criteria Forum	http://www.commoncriteriaforum.org/
CCIF	Cloud Computing Interoperability Forum		Standard and Interoperability Working Group	http://www.cloudforum.org/
CCIF	Cloud Computing Interoperability Forum		Unified Cloud Interface Working Group	http://code.google.com/p/unifiedcloud/
CIE	Chinese Institute of Electronics	CCEA	Cloud Computing Experts Association	http://www.ciecloud.org/
CSA	Cloud Security Alliance	CloudAudit	Cloud Audit Working group	https://cloudsecurityalliance.org/research/cloudaudit/

Abbreviation	Forum Name	SubGroup	SubGroup Name	SubGroup URL
CSA	Cloud Security Alliance	TWG	Telecom Working Group	https://cloudsecurityalliance.org/research/telecom/
CSA	Cloud Security Alliance	SecaaS	Security as a Service Working Group	https://cloudsecurityalliance.org/research/secaas/
CSA	Cloud Security Alliance	CSA Mobile	Mobile Working Group	https://cloudsecurityalliance.org/research/mobile/
CSA	Cloud Security Alliance	Security Guidance	Security Guidance Initiative Working Group	https://cloudsecurityalliance.org/research/security-guidance/
CSA	Cloud Security Alliance	CSA Innovate	Innovation Initiative Working Group	https://cloudsecurityalliance.org/research/innovation/
CSA	Cloud Security Alliance	GRC	GRC Stack Working Group	https://cloudsecurityalliance.org/research/grc-stack/
CSA	Cloud Security Alliance	CAI	Consensus Assessments Initiative Working Group	https://cloudsecurityalliance.org/research/cai/
CSA	Cloud Security Alliance	CCM	Cloud Controls Matrix Working Group	https://cloudsecurityalliance.org/research/ccm/
CSA	Cloud Security Alliance	CTP	CloudTrust Protocol Working Group	https://cloudsecurityalliance.org/research/ctp/
CSA	Cloud Security Alliance	CDG	Cloud Data Governance Working Group	https://cloudsecurityalliance.org/research/cdg/
CSA	Cloud Security Alliance	TCI	Trusted Cloud Initiative Working Group	https://cloudsecurityalliance.org/research/tci/
CSA	Cloud Security Alliance	HIM	Health Information Management Working Group	https://cloudsecurityalliance.org/research/him/
CSA	Cloud Security Alliance	Top Threats	Top Threats to Cloud Computing Working Group	https://cloudsecurityalliance.org/research/top-threats/
CSA	Cloud Security Alliance	Cloud SIRT	CloudSIRT Working Group	https://cloudsecurityalliance.org/research/cloudsirt/
CSA	Cloud Security Alliance	MWG	Cloud Metrics Working Group	http://www.cloudforum.org/
	Cloud Standards Coordination			http://Cloud-standards.org/wiki/
CCSA	China Communications Standards Association	WG1	Network protocol system and Device workgroup	http://www.ccsa.org.cn/
CCSA	China Communications Standards Association	WG4	New Technology and International Standards Workgroup	http://www.ccsa.org.cn/
CCSA	China Communications Standards Association		Mobile Internet Application and Terminal Technical Committee	http://www.ccsa.org.cn/english/tc.php?tcid=tc11
CSCC	Cloud Standards Customer Council		Financial Services	http://www.Cloud-council.org
CSCC	Cloud Standards Customer Council		Government	http://www.Cloud-council.org

Abbreviation	Forum Name	SubGroup	SubGroup Name	SubGroup URL
CSCC	Cloud Standards Customer Council		Healthcare	http://www.Cloud-council.org
CSCC	Cloud Standards Customer Council		Practical Guide	http://www.Cloud-council.org
CSCC	Cloud Standards Customer Council		Security	http://www.Cloud-council.org
CSCC	Cloud Standards Customer Council		XaaS	http://www.Cloud-council.org
DMTF	Distributed Management Task Force		Technical Committee	http://www.dmtf.org/about/working-groups
DMTF	Distributed Management Task Force		Interoperability Committee	http://www.dmtf.org/about/working-groups
DMTF	Distributed Management Task Force		Process and Incubation Committee	http://www.dmtf.org/about/working-groups
ENISA	European Network and Information Security Agency	SAS	Secure Applications and Services	http://www.enisa.europa.eu/activities/application-security
ETSI	European Telecommunications Standards Institute	TC CLOUD	Cloud	http://portal.etsi.org/portal/server.pt/community/3GPP/296?tbId=651
ETSI	European Telecommunications Standards Institute	TC LI	Lawful Interception and Retained Data	http://portal.etsi.org/portal/server.pt/community/3GPP/296?tbId=654
ETSI	European Telecommunications Standards Institute	TC ATTM	Access, Terminals, Transmission and Multiplexing	http://portal.etsi.org/portal/server.pt/community/ATTM/297
GICTF	Global Inter-Cloud Technology Forum		Technology Task Force	http://www.gictf.jp/index_e.html
GICTF	Global Inter-Cloud Technology Forum		Service Useage Task Force	http://www.gictf.jp/index_e.html
GSC	Global Standards Collaboration		Plenary	http://www.gsc16.ca/english/index.html
GSMA	GSM Association	GSM-IREG	Inter-Working, Roaming Expert Group	http://www.gsma.com/working-groups/
GSMA	GSM Association		The Security Group	http://www.gsma.com/working-groups/
GSMA	GSM Association	GSM-TSG	Terminal Steering Group	http://www.gsma.com/working-groups/
IEEE	Institute of Electrical and Electronics Engineers	P2301	Cloud Profiles WG (CPWG) Working Group	http://standards.ieee.org/develop/wg/CPWG-2301_WG.html

Abbreviation	Forum Name	SubGroup	SubGroup Name	SubGroup URL
IEEE	Institute of Electrical and Electronics Engineers	P2302	Intercloud WG (ICWG) Working Group	http://standards.ieee.org/develop/wg/ICWG-2302_WG.html
IETF	Internet Engineering Task Force	appsawg	Applications Area Working Group	http://datatracker.ietf.org/wg/appsawg/
IETF	Internet Engineering Task Force	lisp	Locator/ID Separation Protocol (lisp)	http://datatracker.ietf.org/wg/lisp/
IETF	Internet Engineering Task Force	armd	Address Resolution for Massive numbers of hosts in the Data center	http://datatracker.ietf.org/wg/armd/
IETF	Internet Engineering Task Force	eman	Energy Management	http://datatracker.ietf.org/wg/eman/
IETF	Internet Engineering Task Force	opsawg	Operations and Management Area Working Group	http://datatracker.ietf.org/wg/opsawg/
IETF	Internet Engineering Task Force	mile	Managed Incident Lightweight Exchange	http://datatracker.ietf.org/wg/mile/
IETF	Internet Engineering Task Force	sacm	Security Content Automation Protocol (SCAP)	https://www.ietf.org/mailman/listinfo/sacm
IETF	Internet Engineering Task Force	scim	Simple Cloud Identity Management BOF	https://www.ietf.org/mailman/listinfo/scim
IETF	Internet Engineering Task Force	cmdi	Cloud Data Management Interface	http://datatracker.ietf.org/wg/decade/
IETF	Internet Engineering Task Force	syslog	Syslog Extension for Cloud Using Syslog Structured Data	http://www.ietf.org/mail-archive/web/syslog/current/maillist.html
IETF	Internet Engineering Task Force	SOP	Service Orchestration and Desciption for Cloud Services	https://www.ietf.org/mailman/listinfo/sop
IETF	Internet Engineering Task Force	Cloud mob	Cloud services mobility	https://www.ietf.org/mailman/listinfo/clouds
ISO/IEC JTC1	International Organization for Standardization	SC06	Telecommunications and information exchange between systems	http://www.iso.org/iso/iso_technical_committee.html?commid=45072
ISO/IEC JTC1	International Organization for Standardization	SC07	Software and systems engineering	http://www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?commid=45086
ISO/IEC JTC1	International Organization for Standardization	SC27	IT Security techniques	http://www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?commid=45306
ISO/IEC JTC1	International Organization for Standardization	SC38	Distributed application platforms and services (DAPS)	http://www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?commid=601355
ITU-T	International Telecommunication Union - Telecommunications Standardization Sector	liaison-JTC1	Information technology	http://www.iso.org/iso/iso_technical_committee?commid=45020
ITU-T	International Telecommunication Union - Telecommunications Standardization Sector	SG02	Operational aspects of service provision and telecommunications management	http://www.itu.int/ITU-T/studygroups/com02/index.asp

Abbreviation	Forum Name	SubGroup	SubGroup Name	SubGroup URL
ITU-T	International Telecommunication Union - Telecommunications Standardization Sector	SG05	Environment and climate change	http://www.itu.int/ITU-T/studygroups/com05/index.asp
ITU-T	International Telecommunication Union - Telecommunications Standardization Sector	SG09	Television and sound transmission and integrated broadband cable networks	http://www.itu.int/ITU-T/studygroups/com09/index.asp
ITU-T	International Telecommunication Union - Telecommunications Standardization Sector	SG11	Signalling requirements, protocols and test specifications	http://www.itu.int/ITU-T/studygroups/com11/index.asp
ITU-T	International Telecommunication Union - Telecommunications Standardization Sector	SG12	Performance, QoS and QoE	http://www.itu.int/ITU-T/studygroups/com12/index.asp
ITU-T	International Telecommunication Union - Telecommunications Standardization Sector	SG13	Future networks including mobile and NGN	http://www.itu.int/ITU-T/studygroups/com13/index.asp
ITU-T	International Telecommunication Union - Telecommunications Standardization Sector	SG15	Optical transport networks and access network infrastructures	http://www.itu.int/ITU-T/studygroups/com15/index.asp
ITU-T	International Telecommunication Union - Telecommunications Standardization Sector	SG16	Multimedia coding, systems and applications	http://www.itu.int/ITU-T/studygroups/com16/index.asp
ITU-T	International Telecommunication Union - Telecommunications Standardization Sector	SG17	Security	http://www.itu.int/ITU-T/studygroups/com17/index.asp
ITU-T	International Telecommunication Union - Telecommunications Standardization Sector	TSAG	Telecommunication Standardization Advisory Group	http://www.itu.int/ITU-T/tsag/index.asp
Metro Ethernet Forum	Metro Ethernet Forum		Technical Committee	http://metroethernetforum.org/page_loader.php?p_id=79
NIST	National Institute of Standards and Technology		Cloud Computing Program	http://www.nist.gov/itl/Cloud/
NIST	National Institute of Standards and Technology		Reference Architecture and Taxonomy Working Group	http://collaborate.nist.gov/twiki-Cloud-computing/bin/view/CloudComputing/ReferenceArchitectureTaxonomy
NIST	National Institute of Standards and Technology		Standards Acceleration to Jumpstart the Adoption of Cloud Computing Working Group	http://collaborate.nist.gov/twiki-Cloud-computing/bin/view/CloudComputing/SAJACC
NIST	National Institute of Standards and Technology		Cloud Security Working Group	http://collaborate.nist.gov/twiki-Cloud-computing/bin/view/CloudComputing/CloudSecurity

Abbreviation	Forum Name	SubGroup	SubGroup Name		SubGroup URL
NIST	National Institute of Standards and Technology		Standards Roadmap Working Group		http://collaborate.nist.gov/twiki-Cloud-computing/bin/view/CloudComputing/StandardsRoadmap
NIST	National Institute of Standards and Technology		CC Business Use Cases Working Group		http://collaborate.nist.gov/twiki-Cloud-computing/bin/view/CloudComputing/BusinessUseCases
NIST	National Institute of Standards and Technology		Useful Documents for Cloud Adopters		http://collaborate.nist.gov/twiki-Cloud-computing/bin/view/CloudComputing/Documents
NIST	National Institute of Standards and Technology		Koala Project		http://collaborate.nist.gov/twiki-Cloud-computing/bin/view/CloudComputing/KoalaProject
OASIS	Organization for the Advancement of Structured Information Standards	ID-CLOUD	Identity in the Cloud TC		http://www.oasis-open.org/committees/id-Cloud/charter.php
OASIS	Organization for the Advancement of Structured Information Standards	TOSCA	Topology and Orchestration Specification for Cloud Applications (TOSCA) TC		http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=tosca
OASIS	Organization for the Advancement of Structured Information Standards		SOA Reference Model TC		http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=soa-rm
OASIS	Organization for the Advancement of Structured Information Standards		PMRM	Privacy Management Reference Model TC	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pmrm
OASIS	Organization for the Advancement of Structured Information Standards		AMQP	Advanced Message Queuing Protocol TC	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=amqp
OASIS	Organization for the Advancement of Structured Information Standards		Transformational Government Framework TC		http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=tgf
OCC	Open Cloud Consortium		OCSD	The Open Science Data Cloud Working Group	http://opencloudconsortium.org/working-groups/
OCC	Open Cloud Consortium			Project Matsu	http://opencloudconsortium.org/working-groups/
OCC	Open Cloud Consortium			OCC Virtual Network Testbed	http://opencloudconsortium.org/working-groups/
OCC	Open Cloud Consortium			Open Cloud Testbed Working Group	http://opencloudconsortium.org/working-groups/
ODCA	Open Data Center Alliance			Infrastructure	http://www.opendatacenteralliance.org/ourwork/technicalworkgroups
ODCA	Open Data Center Alliance			Management	http://www.opendatacenteralliance.org/ourwork/technicalworkgroups
ODCA	Open Data Center Alliance			Regulation and Ecosystem	http://www.opendatacenteralliance.org/ourwork/technicalworkgroups

Abbreviation	Forum Name	SubGroup	SubGroup Name		SubGroup URL
ODCA	Open Data Center Alliance			Security	http://www.opendatacenteralliance.org/ourwork/technicalworkgroups
ODCA	Open Data Center Alliance			Services	http://www.opendatacenteralliance.org/ourwork/technicalworkgroups
OGF	Open Grid Forum			Applications Working Groups	http://www.ogf.org/gf/group_info/areasgroups.php?area_id=5
OGF	Open Grid Forum			Architecture Working Groups	http://www.ogf.org/gf/group_info/areasgroups.php?area_id=4
OGF	Open Grid Forum			Compute Working Groups	http://www.ogf.org/gf/group_info/areasgroups.php?area_id=3
OGF	Open Grid Forum			Data Working Groups	http://www.ogf.org/gf/group_info/areasgroups.php?area_id=2
OGF	Open Grid Forum			Infrastructure Working Groups	http://www.ogf.org/gf/group_info/areasgroups.php?area_id=1
OGF	Open Grid Forum			Liaison Working Group	http://www.ogf.org/gf/group_info/areasgroups.php?area_id=8
OGF	Open Grid Forum			Management Working Groups	http://www.ogf.org/gf/group_info/areasgroups.php?area_id=6
OGF	Open Grid Forum			Security Working Groups	http://www.ogf.org/gf/group_info/areasgroups.php?area_id=7
OGF	Open Grid Forum		OCCI	Open Cloud Computing Interface Working Group	http://occi-wg.org/
OMA	Open Mobile Alliance		ARC	Architecture Working Group	http://www.openmobilealliance.org/Technical/arc.aspx
OMA	Open Mobile Alliance		BCASR	Broadcasting Working Group	http://www.openmobilealliance.org/Technical/bcast.aspx
OMA	Open Mobile Alliance		COM	Communications Working Group	http://www.openmobilealliance.org/Technical/com.aspx
OMA	Open Mobile Alliance		CD	Content Delivery Working Group	http://www.openmobilealliance.org/Technical/cd.aspx
OMA	Open Mobile Alliance		DM	Device Management Working Group	http://www.openmobilealliance.org/Technical/DM.aspx
OMA	Open Mobile Alliance		DRM	Digital Rights Management Working Group	http://www.openmobilealliance.org/Technical/DRM.aspx
OMA	Open Mobile Alliance		IOP	Interoperability Working Group	http://www.openmobilealliance.org/Technical/IOP.aspx

Abbreviation	Forum Name	SubGroup	SubGroup Name		SubGroup URL
OMA	Open Mobile Alliance		LOC	Location Working Group	http://www.openmobilealliance.org/Technical/LOC.aspx
OMA	Open Mobile Alliance		REL	Release Planning and Management Committee	http://www.openmobilealliance.org/Technical/rel.aspx
OMA	Open Mobile Alliance		REQ	Requirements Working Group	http://www.openmobilealliance.org/Technical/req.aspx
OMG	Object Management Group			Telecommunications PSIG	http://telecom.omg.org/
Open Group	The Open Group			Cloud Computing Work Group	http://www3.opengroup.org/getinvolved/workgroups/cloudcomputing
Open Group	The Open Group			Service-Oriented Architecture Work Group	http://www3.opengroup.org/standards/soa
Open Group	The Open Group			Security Forum	http://www3.opengroup.org/getinvolved/forums/security
Open Group	The Open Group		OTTF	Trusted Technology Forum	http://www3.opengroup.org/getinvolved/forums/trusted
SNIA	Storage Networking Industry Association		ABDC	Analytics and Big Data Committee	http://www.snia.org/forums/abdc
SNIA	Storage Networking Industry Association		CSI	The Cloud Storage Initiative	http://www.snia.org/forums/csi
SNIA	Storage Networking Industry Association		DPCO	Data Protection and Capacity Optimization Committee	http://www.snia.org/forums/dpco
SNIA	Storage Networking Industry Association		ESF	Ethernet Storage Forum	http://www.snia.org/forums/esf
SNIA	Storage Networking Industry Association		GSI	Green Storage Initiative	http://www.snia.org/forums/green
SNIA	Storage Networking Industry Association		SMI	Storage Management Initiative	http://www.snia.org/forums/smi
SNIA	Storage Networking Industry Association		SSIF	Storage Security Industry Forum	http://www.snia.org/forums/ssif
SNIA	Storage Networking Industry Association		XAM	XAM Initiative	http://www.snia.org/forums/xam
TCG	Trusted Computing Group			Authentication Work Group	http://www.trustedcomputinggroup.org/solutions/authentication

Abbreviation	Forum Name	SubGroup	SubGroup Name		SubGroup URL
TCG	Trusted Computing Group			Infrastructure Work Group	http://www.trustedcomputinggroup.org/developers/infrastructure
TCG	Trusted Computing Group		MTM	Mobile Phone Work Group	http://www.trustedcomputinggroup.org/developers/mobile
TCG	Trusted Computing Group			PC Client Work Group	http://www.trustedcomputinggroup.org/developers/pc_client
TCG	Trusted Computing Group			Server Work Group	http://www.trustedcomputinggroup.org/developers/server
TCG	Trusted Computing Group			Storage Work Group	http://www.trustedcomputinggroup.org/developers/storage
TCG	Trusted Computing Group		TMI	Trusted Multi-tenant Infrastructure Work Group	http://www.trustedcomputinggroup.org/developers/trusted_multitenant_infrastructure
TCG	Trusted Computing Group		TNC	Trusted Network Connect Work Group	http://www.trustedcomputinggroup.org/developers/trusted_network_connect
TCG	Trusted Computing Group		TPM	Trusted Platform Module Work Group	http://www.trustedcomputinggroup.org/developers/trusted_platform_module
TCG	Trusted Computing Group		TSS	TCG Software Stack Work Group	http://www.trustedcomputinggroup.org/developers/software_stack
TCG	Trusted Computing Group		VPWG	Virtualized Platform Work Group	http://www.trustedcomputinggroup.org/developers/virtualized_platform
TMForum	TeleManagement Forum		TMForum	Enterprise Cloud Leadership Council	http://www.tmforum.org/EnterpriseCloudLeadership/8009/home.html
TMForum	TeleManagement Forum			Cloud & New Services Initiatve	http://www.tmforum.org/EnablingCloudServices/8006/home.html
TMForum	TeleManagement Forum		TAM	Application Framework Domain	http://www.tmforum.org/ApplicationFramework/10819/home.html
TMForum	TeleManagement Forum		eTOM	Business Process Framework Domain	http://www.tmforum.org/BusinessProcessFramework/8175/Home.html
TMForum	TeleManagement Forum		SID	Information Framework Domain	http://www.tmforum.org/InformationFramework/10817/home.html
TMForum	TeleManagement Forum			Integration Framework Domain	http://www.tmforum.org/IntegrationFramework/10818/home.html
TMForum	TeleManagement Forum			Revenue Assurance Solution Domain	http://www.tmforum.org/Guidebooks/GB941RevenueAssurance/45341/article.html
TMForum	TeleManagement Forum			Enabling New Services Initiative	http://www.tmforum.org/EnablingCloudServices/8006/home.html

History

Document history		
V1.1.1	January 2016	Publication